

# Assisted Common Information with an Application to Secure Two-Party Sampling

Vinod M. Prabhakaran

Tata Institute of Fundamental Research, India

Email: vinodmp@tifr.res.in

Manoj M. Prabhakaran

University of Illinois, Urbana-Champaign, USA

Email: mmp@illinois.edu

**Abstract**—Secure multi-party computation is a central problem in modern cryptography. An important sub-class of this are problems of the following form: Alice and Bob desire to produce sample(s) of a pair of jointly distributed random variables. Each party must learn nothing more about the other party’s output than what its own output reveals. To aid in this, they have available a *set up* — correlated random variables whose distribution is different from the desired distribution — as well as unlimited noiseless communication. In this paper we present an upperbound on how efficiently a given set up can be used to produce samples from a desired distribution.

The key tool we develop is called *tension* — or more precisely, the *region of tension* — which measures how well the correlation between a pair of random variables can be (or rather, cannot be) resolved as a piece of common information and other independent pieces of information. We show various properties of this region, including a crucial monotonicity property: *a protocol between two parties can only lower the tension between their views* (i.e., a (low) level of tension that used to be achievable before the protocol remains achievable after it, along with possibly new lower levels). Then, by calculating the bounds on the region of tension of various pairs of correlated random variables, we derive state-of-the-art bounds on the efficiency of producing samples from a desired distribution using a given set up.

Another important contribution of this work is to generalize the notion of common information of two dependent variables introduced by [Gács-Körner, 1973]. They defined common information as the largest entropy rate of a common random variable two parties observing one of the sources each can agree upon. It is well-known that their common information captures only a limited form of dependence between the random variables and is zero in most cases of interest. Our generalization, which we call the *Assisted Common Information* system, lets us take into account “almost common” information

ignored by Gács-Körner common information. In the assisted common information system, a genie assists the parties in agreeing on a more substantial common random variable; we characterize the trade-off between the amount of communication from the genie and the quality of the common random variable produced. We show that the optimal trade-off is essentially given by the region of tension. Connections to the Gray-Wyner system and Wyner’s common information are also studied.

## I. INTRODUCTION

Secure multi-party computation is a central problem in modern cryptography. Roughly, the goal of secure multi-party computation is to carry out computations on inputs distributed among two (or more) parties, so as to provide each of them with no more information than what their respective inputs and outputs reveal to them. Our focus in this paper is on an important sub-class of such problems — which we shall call *secure 2-party sampling* — in which the computation has no inputs, but the outputs to the parties are required to be from a given joint distribution (and each party should not learn anything more than its part of the output). Also we shall restrict ourselves to the case of honest-but-curious adversaries. It is well-known (see, for instance, [30] and references therein) that very few distributions can be sampled from in this way, unless the computation is aided by a *set up* — some correlated random variables that are given to the parties at the beginning of the protocol. The set up itself will be from some distribution  $(X, Y)$  (Alice gets  $X$  and Bob gets  $Y$ ) which is different from the desired distribution  $(U, V)$  (Alice getting  $U$  and Bob getting  $V$ ). The fundamental question then is, which set ups  $(X, Y)$  can be used to securely sample which distributions  $(U, V)$ , and *how efficiently*.

While the feasibility question can be answered using combinatorial analysis (as, for instance, was done in

[19]), information theoretic tools have been put to good use to show bounds on efficiency of protocols (e.g. [2], [7], [27], [15], [12], [5], [13], [29], [26]). Our work continues on this vein of using information theory to formulate and answer efficiency questions in cryptography. Specifically, we generalize the concept of common information [9] as defined by Gács and Körner (GK) and use this generalization to establish upper bounds on the efficiency of secure sampling.

Finding a meaningful definition for the “common information” of a pair of dependent random variables  $X$  and  $Y$  has received much attention starting from the 1970s [9], [28], [31], [1], [33]. We propose a new measure — a three-dimensional region — which brings out a detailed picture of the extent of common information of a pair. This gives us an expressive means to compare different pairs with each other, based on the shape and size of their respective regions. Besides the specific application to secure sampling discussed in this paper, we believe that our generalization may potential applications in information theory, cryptography, game theory, and distributed control, where the role of dependent random variables and common randomness is well-recognized.

Suppose  $X = (X', Q)$  and  $Y = (Y', Q)$  where  $X', Y', Q$  are independent. Then a natural measure of “common information” of  $X$  and  $Y$  is  $H(Q)$ .  $Q$  is determined both by  $X$  and by  $Y$ , and further, conditioned on  $Q$ , there is no “residual information” that correlates  $X$  and  $Y$  i.e.,  $X - Q - Y$ . One could extend this to arbitrary  $X, Y$ , in a couple of natural ways. One approach, which corresponds to a definition of Gács and Körner [9]<sup>1</sup> is to find the “largest” random variable  $Q$  that is determined by  $X$  alone as well as by  $Y$  alone (with probability 1):

$$\begin{aligned} C_{\text{GK}}(X; Y) &= \max_{\substack{p_{Q|XY}: \\ H(Q|X)=H(Q|Y)=0}} H(Q) \\ &= I(X; Y) - \min_{\substack{p_{Q|XY}: \\ H(Q|X)=H(Q|Y)=0}} I(X; Y|Q). \end{aligned} \quad (1)$$

Note that in this case, the common information is necessarily no more than the mutual information, and in general this gap is non-zero, i.e., common information, in general, does not account for all the correlation between  $X$  and  $Y$ . An alternate generalization, which corresponds to the approach of Gray and Wyner [31]<sup>2</sup> is to consider

the “smallest” random variable  $Q$  so that conditioned on  $Q$  there is no residual mutual information. Smallness of  $Q$ , in this case is measured in terms of  $I(XY; Q)$ .

$$\begin{aligned} C_{\text{Wyner}}(X; Y) &= \min_{\substack{p_{Q|XY}: \\ X-Q-Y}} I(XY; Q) \\ &= I(X; Y) + \min_{\substack{p_{Q|XY}: \\ X-Q-Y}} (I(Y; Q|X) + I(X; Q|Y)). \end{aligned} \quad (2)$$

Note that in this case, the common information is necessarily no less than the mutual information. When  $X, Y$  are of the form  $X = (X', Q)$  and  $Y = (Y', Q)$ , where  $X', Y', Q$  are independent, then there indeed is a unique interpretation of common information (when  $C_{\text{GK}}(X; Y) = C_{\text{Wyner}}(X; Y) = H(Q)$ ). But otherwise, between the extremes represented by these two measures, there are several ways in which one could define a random variable to capture the correlation between  $X$  and  $Y$ .

One way to look at the new quantities we introduce is as a way to capture an entire spectrum of random variables that approximately capture the correlation between  $X$  and  $Y$ . In Section II we shall define a three-dimensional “region of tension” for  $X, Y$ , which measures how well can the correlation between  $X, Y$  be captured by a random variable. In Figure 1 we schematically depict this region. Looking ahead, we mark the quantities  $I(X; Y) - C_{\text{GK}}(X; Y)$  and  $C_{\text{Wyner}}(X; Y) - I(X; Y)$  there in this figure, to illustrate the gap between mutual information and the two notions of common information in terms of the region of tension.

In Section III, we generalize the Gács-Körner system in terms of which  $C_{\text{GK}}$  is defined (see Figure 4) to the “Assisted Common Information system.” We show that the associate rate regions are closely related to the region of tension (Corollary 3.2). In Section IV, we consider the Gray-Wyner system (which gives a generalization of  $C_{\text{Wyner}}$ ) and show that the rate region associated with this system is also closely related to the region of tension (Theorem 4.3). This clarifies the connection between  $C_{\text{GK}}$  and the Gray-Wyner system. In particular, previously known connections readily follow from our results. Further, we show how two quantities identified in recent work in the context of lossless coding with side-information [20] and the Gray-Wyner system [17] can be obtained in terms of the region of tension (Corollary 4.6).

Quite apart from the information theoretic questions related to common information, our motivating application for defining the region of tension is the cryptographic problem of bounding the efficiency of secure-sampling described above. In Section V, we show that the region of tension of the views of two parties engaged in such a protocol can only monotonically lower (expand

<sup>1</sup>This is not the *definition* of common information in [9], but the consequence of a non-trivial result in that work. The original definition, which is in terms of a communication problem, is detailed in Section III (along with our extensions).

<sup>2</sup>Again, the actual definition of [31], which is in terms of a source coding problem, is different. The expression above is a consequence of a result in [31]. The definition and results in [31] are described in Section IV.

towards the origin) and not rise (shrink away from the origin). Thus, by comparing the regions for the target random variables and the given random variables, we obtain improved upperbounds on the efficiency with which one pair can be used to securely generate another pair. We also give an example where this upperbound strictly improves on the prior work, but is further interesting for two reasons: firstly, this example is based on natural correlated random variables that are widely studied (namely, variants of oblivious transfer), and secondly the new upperbound we can prove actually matches an easy lowerbound and is therefore tight.

*Outline:* Section II defines the region of tension for a pair of correlated random variables, and establishes some of its properties. Section III and Section IV introduce the concepts of common information  $C_{\text{GK}}$  and  $C_{\text{Wyner}}$  in terms of the Gács-Körner and Gray-Wyner systems (and a new generalization, in the case of the former), and establishes the connections with the region of tension. Section V defines the secure sampling problem, a monotonicity property of the region of tension and its application in bounding the efficiency of secure sampling. The reader may choose to read only Section II, Section III and Section IV, or alternately only Section II and Section V.

## II. TENSION AND THE REGION OF TENSION

Now we introduce our main tool which generalizes GK common information and also serves as a measure of cryptographic complexity of securely sampling a pair of random variables. Intuitively, we measure how well common information captures (or does not capture) the mutual information between a pair of random variables  $(X, Y)$ .

### A. Definitions

Throughout this paper we concern ourselves with pairs of correlated *finite* random variables  $(X, Y)$  with joint distribution (p.m.f.)  $p_{X,Y}$ .  $\mathcal{X}$  and  $\mathcal{Y}$  shall stand for the (finite) alphabets of  $X$  and  $Y$  respectively. We let  $\mathcal{P}_{X,Y}$  denote the set of all random variables  $Q$  jointly distributed with  $(X, Y)$  — i.e., all conditional p.m.f.s  $p_{Q|X,Y}$ .

The *total variation distance*<sup>3</sup> between two random variables  $X$  and  $X'$  over the same alphabet  $\mathcal{X}$  is  $\Delta(X, X') \triangleq \frac{1}{2} \|p_X - p_{X'}\|_1 = \frac{1}{2} \sum_{x \in \mathcal{X}} |p_X(x) - p_{X'}(x)|$ .  $H_2(\cdot)$  will denote the binary entropy function:  $H_2(p) \triangleq p \log(1/p) + (1-p) \log(1/(1-p))$  (for  $0 < p < 1$ ), and  $H_2(0) = H_2(1) = 0$ .

<sup>3</sup>In cryptography literature,  $\Delta(\cdot, \cdot)$  is more commonly called statistical difference.

The *characteristic bipartite graph* of a pair of correlated random variables  $(X, Y)$  is the graph with vertices in  $\mathcal{X} \cup \mathcal{Y}$  and an edge between  $x \in \mathcal{X}$  and  $y \in \mathcal{Y}$  if and only if  $p_{XY}(x, y) > 0$ . (See Figure 3 for an example.)

Now we give the main definitions of this section.

*Definition 2.1:* For a pair of correlated random variables  $(X, Y)$ , and  $p_{Q|XY} \in \mathcal{P}_{X,Y}$ , we say  $Q$  *perfectly resolves*  $(X, Y)$  if  $I(X; Y|Q) = 0$  and  $H(Q|X) = H(Q|Y) = 0$ . We say  $(X, Y)$  is *perfectly resolvable* if there exists  $p_{Q|XY} \in \mathcal{P}_{X,Y}$  such that  $Q$  perfectly resolves  $(X, Y)$ .

If  $(X, Y)$  is perfectly resolvable, then their GK common information represents the entire mutual information between them (see (1)). We intend to measure the extent to which  $(X, Y)$  is *not* perfectly resolvable. Towards this we introduce a 3-dimensional measure called *tension* of  $(X, Y)$ , defined as follows.

*Definition 2.2:* For a pair of correlated random variables  $(X, Y)$  and  $p_{Q|XY} \in \mathcal{P}_{X,Y}$ , the *tension* of  $(X, Y)$  given  $Q$  is denoted by  $T(X; Y|Q) \in \mathbb{R}_+^3$  and defined as  $T(X; Y|Q) \triangleq (I(Y; Q|X), I(X; Q|Y), I(X; Y|Q))$ . The *region of tension* of  $(X, Y)$ , denoted by  $\mathfrak{T}(X; Y) \subseteq \mathbb{R}_+^3$  is defined as

$$\mathfrak{T}(X; Y) \triangleq i(\{T(X; Y|Q) : p_{Q|XY} \in \mathcal{P}_{X,Y}\}),$$

where  $i(S)$  denotes the *increasing hull* of  $S \subseteq \mathbb{R}_+^3$ , defined as  $i(S) \triangleq \{s \in \mathbb{R}_+^3 : \exists s' \in S \text{ s.t. } s \geq s'\}$ .<sup>4</sup>

Since we consider only random variables with finite alphabets  $\mathcal{X}$  and  $\mathcal{Y}$ , it follows from Fenchel-Eggleston's strengthening of Carathéodory's theorem [6, pg. 310], that we can restrict ourselves to  $p_{Q|XY} \in \mathcal{P}_{X,Y}$  with alphabet  $\mathcal{Q}$  such that  $|\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}| + 2$ . More precisely,

$$\mathfrak{T}(X; Y) = i\left(\{T(X; Y|Q) : p_{Q|XY} \in \widehat{\mathcal{P}}_{X,Y}\}\right), \quad (3)$$

where  $\widehat{\mathcal{P}}_{X,Y}$  is defined as the set of all conditional p.m.f.'s  $p_{Q|X,Y}$  such that the cardinality of alphabet  $\mathcal{Q}$  of  $Q$  is such that  $|\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}| + 2$ .

We point out that  $\mathfrak{T}(X; Y)$  intersects all three axes (e.g., consider  $Q = Y$ ,  $Q = X$  and  $Q = 0$ , respectively). It will be of interest to consider the three axes intercepts of the boundary of  $\mathfrak{T}(X; Y)$ .

$$\begin{aligned} T_1^{\text{int}}(X; Y) &\triangleq \min\{r_1 : (r_1, 0, 0) \in \mathfrak{T}(X; Y)\} \\ T_2^{\text{int}}(X; Y) &\triangleq \min\{r_2 : (0, r_2, 0) \in \mathfrak{T}(X; Y)\} \\ T_3^{\text{int}}(X; Y) &\triangleq \min\{r_3 : (0, 0, r_3) \in \mathfrak{T}(X; Y)\} \end{aligned} \quad (4)$$

The use of min instead of inf anticipates Theorem 2.4 which shows that  $\mathfrak{T}(X; Y)$  is closed.

<sup>4</sup>For two vectors  $(x, y, z), (x', y', z') \in \mathbb{R}_+^3$ , we write  $(x, y, z) \geq (x', y', z')$  to mean  $x \geq x'$ ,  $y \geq y'$  and  $z \geq z'$ .

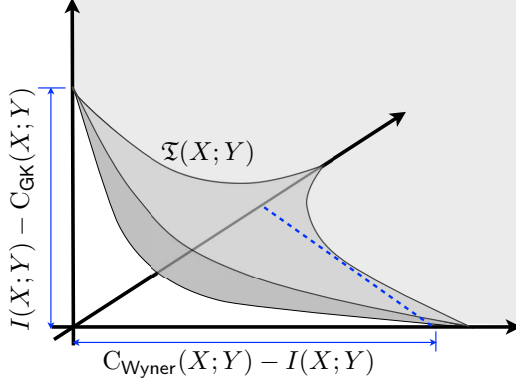


Fig. 1: A schematic representation of the region  $\mathfrak{T}(X; Y)$ .  $\mathfrak{T}(X; Y)$  is an unbounded, convex region, bounded away from the origin (unless  $(X, Y)$  is perfectly resolvable). Relationship between two points on the boundary of  $\mathfrak{T}(X; Y)$  and the quantities  $C_{GK}(X; Y)$  and  $C_{Wyner}(X; Y)$  (see (16) and (34)) is shown. (The dotted line is at  $45^\circ$  to the axes.)

### B. Some Properties of Tension

Firstly, we have an easy observation.

**Theorem 2.1:**  $\mathfrak{T}(X; Y)$  includes the origin if and only if the pair  $(X, Y)$  is perfectly resolvable.

*Proof:* We need to show that there exists  $p_{Q|XY}$  such that  $I(Y; Q|X) = I(X; Q|Y) = I(X; Y|Q) = 0$  if and only if there exists  $p_{Q'|XY}$  such that  $H(Q'|X) = H(Q'|Y) = I(X; Y|Q') = 0$ . Clearly, the second condition implies the first by taking  $Q$  to be the same as  $Q'$ . The converse follows from Lemma A.1 which shows that given  $p_{Q|XY}$  such that  $I(Y; Q|X) = I(X; Q|Y) = 0$ , we can find a random variable  $Q'$  with  $H(Q'|X) = H(Q'|Y) = 0$  and  $Q - Q' - XY$ ; then, by Lemma A.2 it follows that  $I(X; Y|Q') \leq I(X; Y|Q)$ , and hence  $I(X; Y|Q) = 0$  implies  $I(X; Y|Q') = 0$ . ■

The more interesting case is when  $\mathfrak{T}(X; Y)$  does not contain the origin, and hence  $(X, Y)$  is not perfectly resolvable. Note that it is important to consider all three coordinates of  $T(X; Y|Q)$  together to identify the unresolvable nature of a pair  $(X, Y)$ , because, as observed above,  $\mathfrak{T}(X; Y)$  does intersect each of the three axes, or in other words, any two coordinates of  $T(X; Y|Q)$  can be made simultaneously 0 by choosing an appropriate  $Q$ .

As it turns out, the axes intercepts are identical to three quantities identified by Wolf and Wullschlegler [29]. In [29] these quantities were defined as

$$H(X \searrow Y|Y) \quad H(Y \searrow X|X) \quad I(X; Y|X \wedge Y)$$

where,  $X \searrow Y$  stands for the part of  $X$  which depends on  $Y$  (i.e., a function of  $X$  which distinguishes between different values of  $X$  if and only if they induce different conditional distributions on  $Y$ ), and  $X \wedge Y$  stands for the *common information* between  $X$  and  $Y$  (i.e., the “maximal” function of  $X$  that is also a function of  $Y$ , as discussed in more detail in Section III). More precisely, the three quantities considered there are such that:

$$H(Y \searrow X|X) = \min_{p_{Q|XY}: H(Q|Y)=I(X; Y|Q)=0} H(Q|X)$$

$$H(X \searrow Y|Y) = \min_{p_{Q|XY}: H(Q|X)=I(X; Y|Q)=0} H(Q|Y)$$

$$I(X; Y|X \wedge Y) = \min_{p_{Q|XY}: H(Q|X)=H(Q|Y)=0} I(X; Y|Q).$$

In the appendix we prove the following theorem that these three quantities are the same as  $(T_1^{\text{int}}(X; Y), T_2^{\text{int}}(X; Y), T_3^{\text{int}}(X; Y))$ .

**Theorem 2.2:**

$$T_1^{\text{int}}(X; Y) = \min_{p_{Q|XY}: H(Q|Y)=I(X; Y|Q)=0} H(Q|X) \quad (5)$$

$$T_2^{\text{int}}(X; Y) = \min_{p_{Q|XY}: H(Q|X)=I(X; Y|Q)=0} H(Q|Y) \quad (6)$$

$$T_3^{\text{int}}(X; Y) = \min_{p_{Q|XY}: H(Q|X)=H(Q|Y)=0} I(X; Y|Q). \quad (7)$$

**Monotonicity of  $\mathfrak{T}(X; Y)$ :** Wolf and Wullschlegler showed that these three quantities have a certain “monotonicity” property (they can only decrease, as  $X, Y$  evolve as the views of two parties in a secure protocol). We shall see that the monotonicity of all the three quantities is a consequence of the monotonicity of the entire region  $\mathfrak{T}(X; Y)$ . We define the precise nature of this monotonicity in Section V-B and prove it for  $\mathfrak{T}(X; Y)$  in Section V-C.

The following result (proven in Appendix A) will be useful in defining a “multiplication” operation on the region of tension as a scaling (see (44)). This in turn would be useful in relating the region of tension and the rate of secure sampling, in Section V.

**Theorem 2.3:** The region  $\mathfrak{T}(X; Y)$  is convex.

In extending the results in Section V to statistical security (rather than perfect security), the following results would be important. Firstly, the region of tension is closed.

**Theorem 2.4:** The region  $\mathfrak{T}(X; Y)$  is closed.

*Proof:* By (3), and the fact that the increasing hull of a compact set is closed (see Lemma A.3 in Appendix A), it is enough to show that  $\{T(X; Y|Q) : p_{Q|XY} \in \hat{\mathcal{P}}_{X,Y}\}$

is compact (i.e., closed and bounded (Heine-Borel theorem)). For this, notice that  $T(X;Y|Q)$  as a function of  $p_{Q|XY}$  – i.e., as a function from  $\hat{\mathcal{P}}_{X,Y}$  to  $\mathbb{R}^3$  – is continuous. Moreover,  $\hat{\mathcal{P}}_{X,Y}$  is compact. Since the image of a compact set under a continuous function is compact,  $\{T(X;Y|Q) : p_{Q|XY} \in \hat{\mathcal{P}}_{X,Y}\}$  is compact. ■

Secondly, the region of tension is *continuous* in the sense that when the joint p.m.f.  $p_{X,Y}$  is close to the joint p.m.f.  $p_{X',Y'}$ , the tension regions  $\mathfrak{T}(X;Y)$  and  $\mathfrak{T}(X';Y')$  are also close. We measure closeness of these two joint p.m.f.'s (assumed without loss of generality to be defined over the same alphabet  $\mathcal{X} \times \mathcal{Y}$ ) by their total variation distance  $\Delta(XY, X'Y')$ .

**Theorem 2.5:** Suppose  $\Delta(XY, X'Y') = \epsilon$ , for some  $\epsilon \in [0, 1]$ . Then,  $\mathfrak{T}(X;Y) \subseteq \mathfrak{T}(X';Y') - \delta(\epsilon)$ , where  $\delta(\epsilon) = 2H_2(\epsilon) + \epsilon \log \max\{|\mathcal{X}|, |\mathcal{Y}|\}$ , and for  $S \in \mathbb{R}^3, \alpha \in \mathbb{R}$ , the notation  $S - \alpha$  stands for  $\{(r_1 - \alpha, r_2 - \alpha, r_3 - \alpha) : (r_1, r_2, r_3) \in S\}$ .

*Proof:* Suppose  $(r_1, r_2, r_3) \in \mathfrak{T}(X;Y)$ . We shall show that  $(r_1 + \delta(\epsilon), r_2 + \delta(\epsilon), r_3 + \delta(\epsilon)) \in \mathfrak{T}(X';Y')$ . Since  $(r_1, r_2, r_3) \in \mathfrak{T}(X;Y)$ , there is a  $p_{Q|X,Y} \in \mathcal{P}_{X,Y}$  such that  $I(Y;Q|X) \leq r_1$ ,  $I(X;Q|Y) \leq r_2$ , and  $I(X;Y|Q) \leq r_3$ . Let  $p_{Q'|X',Y'} = p_{Q|X,Y}$ . It is enough to prove that

$$\begin{aligned} I(Y';Q'|X') &\leq I(Y;Q|X) + \delta(\epsilon), \\ I(X';Q'|Y') &\leq I(X;Q|Y) + \delta(\epsilon), \\ I(X';Y'|Q') &\leq I(X;Y|Q) + \delta(\epsilon). \end{aligned}$$

We will make use of the following lemma which is proved in Appendix A.

**Lemma 2.6:** Suppose random variables  $(A, B, C)$  and  $(A', B', C')$  over the same alphabet  $\mathcal{A} \times \mathcal{B} \times \mathcal{C}$  are such that  $\Delta(ABC, A'B'C') = \epsilon$ . Then  $I(A';B'|C') \leq I(A;B|C) + 2H_2(\epsilon) + \epsilon \log \min\{|\mathcal{A}|, |\mathcal{B}|\}$ .

Note that since  $p_{Q'|X',Y'} = p_{Q|X,Y}$ , we have  $\Delta(XYQ, X'Y'Q') = \Delta(XY, X'Y') = \epsilon$ . Then we invoke Lemma 2.6 thrice (with  $(ABC, A'B'C')$  standing for  $(YQX, Y'Q'X')$ ,  $(XQY, X'Q'Y')$  and  $(XYQ, X'Y'Q')$ , respectively). This combined with the fact that  $\min\{|\mathcal{Y}|, |\mathcal{Q}|\}$ ,  $\min\{|\mathcal{X}|, |\mathcal{Q}|\}$ ,  $\min\{|\mathcal{X}|, |\mathcal{Y}|\}$ , are all upperbounded by  $\max\{|\mathcal{X}|, |\mathcal{Y}|\}$ , we obtain the requisite bounds. ■

### C. A Few Examples

Obtaining closed form expressions for the region  $\mathfrak{T}(X;Y)$  can be difficult. However, for our applications it often suffices to identify parts of the boundary of

$\mathfrak{T}(X;Y)$ . We give a couple of examples below. A more detailed example appears in Section V-E.

**Example 2.1:** Figure 2 shows the joint p.m.f. of a pair of dependent random variables  $X, Y$ .

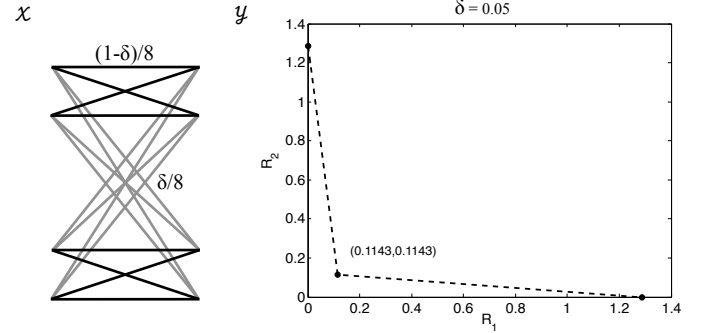


Fig. 2:  $X, Y$  are dependent random variables whose joint p.m.f. is shown. The solid black lines each carry a probability mass of  $\frac{1-\delta}{8}$  and the lighter ones  $\frac{\delta}{8}$ . In the plot, all points  $(R_1, R_2)$  on the dotted lines are such that  $(R_1, R_2, 0) \in \mathfrak{T}(X;Y)$ .

When  $\delta = 0$ , they have the simple dependency structure of  $X = (X', Q), Y = (Y', Q)$  where  $X', Y', Q$  are independent. This is the trivial case in the introduction, and the observers can each produce, without any assistance from the genie,  $Q$  which renders their observations conditionally independent. Thus, the set of rate pairs  $(R_1, R_2)$  such that  $(R_1, R_2, 0) \in \mathfrak{T}(X;Y)$  is the entire positive quadrant. For small values of  $\delta$  we intuitively expect the random variables to be “close” to this case. A measure such as the common information of Gács and Körner fails to bring this out (common information is discontinuous in  $\delta$  jumping from  $H(Q) = 1$  at  $\delta = 0$  to 0 for  $\delta > 0$ ). However, the intuition is borne out by our trade-off regions. For instance, for  $\delta = 0.05$ , Figure 2 shows that the set of rate pairs  $(R_1, R_2)$  such that  $(R_1, R_2, 0) \in \mathfrak{T}(X;Y)$  is nearly all of the positive quadrant.

**Example 2.2: A binary example.** Figure 3 shows the joint p.m.f. of a pair of dependent binary random variables  $U, V$ . In the plot in Figure 3 we show the intersection of  $\mathfrak{T}(U;V)$  with the plane  $z = 0$ .

## III. ASSISTED COMMON INFORMATION

Recall that when  $X = (X', Q)$  and  $Y = (Y', Q)$  where  $X', Y', Q$  are independent, then a natural measure of “common information” of  $X$  and  $Y$  is  $H(Q)$ . In this case, an observer of  $X$  and an observer of  $Y$  may independently produce the common part  $Q$ ; and conditioned on  $Q$ , there is no “residual information” that correlates  $X$  and  $Y$  i.e.,  $I(X;Y|Q) = 0$ . The definition  $C_{\text{GK}}(X;Y)$  of Gács and Körner [9] generalizes this to

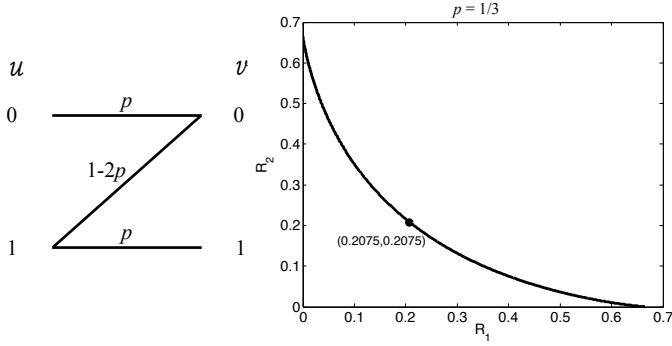


Fig. 3:  $U, V$  are binary random variables with joint p.m.f.  $p(0,0) = p(1,1) = p$ ,  $p(1,0) = 1 - 2p$ , and  $p(0,1) = 0$ . Boundary of the set of all rate pairs  $(R_1, R_2)$  such that  $(R_1, R_2, 0) \in \mathfrak{T}(U; V)$  for  $p = 1/3$  is shown. The marked point is the minimum sum-rate point.

arbitrary  $X, Y$  (Figure 4(a)): the two observers now see  $X^n = (X_1, \dots, X_n)$  and  $Y^n = (Y_1, \dots, Y_n)$ , resp., where  $(X_i, Y_i)$  pairs are independent drawings of  $(X, Y)$ . They are required to produce random variables  $W_1 = f_1(X^n)$  and  $W_2 = f_2(Y^n)$ , resp., which agree (with high probability). The largest entropy rate (i.e., entropy normalized by  $n$ ) of such a “common” random variable was proposed as the *common information* of  $X$  and  $Y$ . We will refer to this as the **GK** common information of  $(X, Y)$  and denote it by  $C_{\text{GK}}(X; Y)$ . However, in the same paper [9], Gács and Körner showed (a result later strengthened by Witsenhausen [28]) that this rate is still just the largest  $H(Q)$  for  $Q$  which can be obtained (with probability 1) as a deterministic function of  $X$  alone as well as a deterministic function of  $Y$  alone.

$$C_{\text{GK}}(X; Y) = \max_{\substack{p_{Q|XY}: \\ H(Q|X)=H(Q|Y)=0}} H(Q).$$

It is easy to see that the above maximum is achieved by the random variable  $Q$  defined over the set of connected components of the characteristic bipartite graph of  $(X, Y)$ , such that  $p_{Q|XY}(q|x, y) = 1$  if and only if the edge  $(x, y)$  belongs to the connected component  $q$ . Note that this captures only an explicit form of common information in a single instance of  $(X, Y)$ .

One limitation of the common information defined by Gács and Körner is that it ignores information which is *almost* common.<sup>5</sup> In particular, if there is only a single connected component in the characteristic bipartite graph then the common information between them is zero, even

<sup>5</sup>Other approaches which do not necessarily suffer from this drawback have been suggested, notably [31], [1], [33]. As we show, our generalization is also intimately connected with [31].

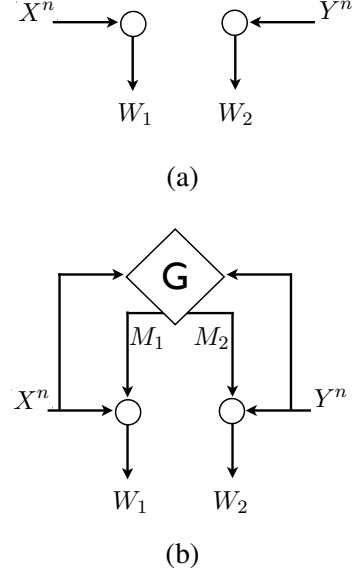


Fig. 4: (a) Setup for Gács-Körner common information. The observers generate  $W_1$  and  $W_2$  which are required to agree with high probability. (b) Assisted common information system. A genie assists the observers by sending separate messages to them over rate-limited noiseless links. When the genie is absent the setup reduces to the one for Gács-Körner common information.

if it is the case that by removing a set of edges that account for a small probability mass, the graph can be disconnected into a large number of components each with a significant probability mass. Our approach in this section could be viewed as a strict generalization of Gács and Körner, which uncovers such extra layers of “almost common information.” Technically, we introduce an omniscient genie who has access to both the observations  $X^n$  and  $Y^n$  and can send separate messages to the two observers over rate-limited noiseless links. See Figure 4(b). The objective is for the observers to agree on a “common” random variable as before, but now with the genie’s assistance. We call this the *assisted common information* system. This leads to a trade-off region trading-off the rates of the noiseless links and the resulting common information<sup>6</sup> (or the resulting residual mutual information). We characterize these trade-off regions in terms of the region of tension of the two random variables, and show that, in general, they exhibit non-trivial behavior, but reduce to the trivial behaviour discussed above when the rates of the noiseless links are zero.

As before, two observers receive  $X^n = (X_1, \dots, X_n)$

<sup>6</sup>We use the term common information primarily to maintain continuity with [9].

and  $Y^n = (Y_1, \dots, Y_n)$  respectively, and need to output strings  $W_1$  and  $W_2$  respectively, that must match each other with high probability. But here, an omniscient Genie  $G$  computes  $M_1 = f_1^{(n)}(X^n, Y^n)$  and  $M_2 = f_2^{(n)}(X^n, Y^n)$  as deterministic functions of  $(X^n, Y^n)$  and sends these to the two observers as shown in Figure 4(b). The observers are allowed to compute their outputs also making use of the respective messages they receive from the genie, as  $W_1 = g_1^{(n)}(X^n, M_1)$  and  $W_2 = g_2^{(n)}(Y^n, M_2)$ , where  $g_1^{(n)}$  and  $g_2^{(n)}$  are deterministic functions. Here again, the goal is to study how large the entropy of  $W_1$  (and equivalently  $W_2$ ) can be, but controlling for the number of bits used to transmit  $M_1$  and  $M_2$ .

For a pair of random variables  $(X, Y)$  and positive integers  $N_1, N_2, n$ , an  $(N_1, N_2, n)$  *assisted common information (ACI) code* is defined as a quadruple  $(f_1^{(n)}, f_2^{(n)}, g_1^{(n)}, g_2^{(n)})$ , where

$$\begin{aligned} f_k^{(n)} : \mathcal{X}^n \times \mathcal{Y}^n &\rightarrow \{1, \dots, N_k\}, \quad k = 1, 2 \\ g_1^{(n)} : \mathcal{X}^n \times \{1, \dots, N_1\} &\rightarrow \mathbb{Z}, \text{ and} \\ g_2^{(n)} : \mathcal{Y}^n \times \{1, \dots, N_2\} &\rightarrow \mathbb{Z} \end{aligned}$$

are deterministic functions. A sequence of  $(N_1(n), N_2(n), n)$  ACI codes  $(f_1^{(n)}, f_2^{(n)}, g_1^{(n)}, g_2^{(n)})_{n=1,2,\dots}$  is called a *valid*  $(R_1, R_2)$  ACI strategy for  $(X, Y)$ , if for every  $\epsilon > 0$ , for sufficiently large  $n$ ,

$$\frac{1}{n} \log N_k(n) \leq R_k + \epsilon, \quad k = 1, 2 \quad (8)$$

$$\Pr[g_1^{(n)}(X^n, f_1^{(n)}(X^n, Y^n)) \neq g_2^{(n)}(Y^n, f_2^{(n)}(X^n, Y^n))] \leq \epsilon. \quad (9)$$

We say that a rate pair  $(R_1, R_2)$  *enables common information rate*  $R_{\text{CI}} \geq 0$  for  $(X, Y)$ , if there exists a valid  $(R_1, R_2)$  ACI strategy  $(f_1^{(n)}, f_2^{(n)}, g_1^{(n)}, g_2^{(n)})_n$  for  $(X, Y)$  such that for every  $\epsilon > 0$ , for sufficiently large  $n$ ,

$$\frac{1}{n} H(g_1^{(n)}(X^n, f_1^{(n)}(X^n, Y^n))) \geq R_{\text{CI}} - \epsilon. \quad (10)$$

Similarly, we say that a rate pair  $(R_1, R_2)$  *enables residual information rate*  $R_{\text{RI}}$  for  $(X, Y)$ , if there exists a valid  $(R_1, R_2)$  ACI strategy  $(f_1^{(n)}, f_2^{(n)}, g_1^{(n)}, g_2^{(n)})_n$  for  $(X, Y)$  such that for every  $\epsilon > 0$ , for sufficiently large  $n$ ,

$$\frac{1}{n} I(X^n; Y^n | g_1^{(n)}(X^n, f_1^{(n)}(X^n, Y^n))) \leq R_{\text{RI}} + \epsilon. \quad (11)$$

Note that if  $(R_1, R_2)$  enables residual information rate  $R_{\text{RI}}$ , and  $(R'_1, R'_2, R'_{\text{RI}}) \geq (R_1, R_2, R_{\text{RI}})$ , then  $(R'_1, R'_2)$  enables residual information rate  $R'_{\text{RI}}$  too.

**Definition 3.1:** The *assisted common information region*  $\mathcal{R}_{\text{ACI}}(X; Y)$  of a pair of correlated random variables

$(X, Y)$  is the set of all  $(R_1, R_2, R_{\text{CI}}) \in \mathbb{R}_+^3$  such that  $(R_1, R_2)$  enables common information rate  $R_{\text{CI}}$  for  $(X, Y)$ . Similarly the *assisted residual information rate region*  $\mathcal{R}_{\text{ARI}}(X; Y)$  of  $(X, Y)$  is the set of all  $(R_1, R_2, R_{\text{RI}}) \in \mathbb{R}_+^3$  such that  $(R_1, R_2)$  enables residual information rate  $R_{\text{RI}}$  for  $(X, Y)$ . In other words,

$$\begin{aligned} \mathcal{R}_{\text{ACI}}(X; Y) &\triangleq \{(R_1, R_2, R_{\text{CI}}) : (R_1, R_2) \text{ enables} \\ &\quad \text{common information rate } R_{\text{CI}} \text{ for } (X, Y)\}, \\ \mathcal{R}_{\text{ARI}}(X; Y) &\triangleq \{(R_1, R_2, R_{\text{RI}}) : (R_1, R_2) \text{ enables} \\ &\quad \text{residual information rate } R_{\text{RI}} \text{ for } (X, Y)\}. \end{aligned}$$

We will write  $\mathcal{R}_{\text{ACI}}$  and  $\mathcal{R}_{\text{ARI}}$  when the random variables involved are obvious from the context. It is easy to see from the definition that  $\mathcal{R}_{\text{ACI}}$  and  $\mathcal{R}_{\text{ARI}}$  are closed sets.

Our main results regarding assisted common information system characterize the assisted residual and common information rate regions of  $(X, Y)$ , and relate them to the region of tension of  $(X, Y)$ .

Recall that  $\hat{\mathcal{P}}_{X,Y}$  is the set of all conditional p.m.f.'s  $p_{Q|X,Y}$  such that the cardinality of alphabet  $\mathcal{Q}$  of  $Q$  is such that  $|\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}| + 2$ . We have the following characterization of the assisted common and residual information regions:

**Theorem 3.1:**

$$\begin{aligned} \mathcal{R}_{\text{ARI}}(X; Y) &= \{(r_1, r_2, r_{\text{RI}}) \in \mathbb{R}_+^3 : \exists p_{Q|X,Y} \in \hat{\mathcal{P}}_{X,Y} \text{ s.t.} \\ &\quad r_1 \geq I(Y; Q|X), r_2 \geq I(X; Q|Y), r_{\text{RI}} \geq I(X; Y|Q)\}. \\ \mathcal{R}_{\text{ACI}}(X; Y) &= \{(r_1, r_2, r_{\text{CI}}) \in \mathbb{R}_+^3 : \exists p_{Q|X,Y} \in \hat{\mathcal{P}}_{X,Y} \text{ s.t.} \\ &\quad r_1 \geq I(Y; Q|X), r_2 \geq I(X; Q|Y), r_{\text{CI}} \leq I(X, Y; Q)\}. \end{aligned}$$

We prove this theorem in Section III-B. An immediate consequence is that we have an interpretation of the region of tension  $\mathfrak{T}(X; Y)$  as the assisted residual information region  $\mathcal{R}_{\text{ARI}}(X; Y)$ . We may also write it down in terms of the assisted common information region:

**Corollary 3.2:** For any pair of correlated random variables  $(X, Y)$ ,

$$\mathfrak{T}(X; Y) = \mathcal{R}_{\text{ARI}}(X; Y) \quad (12)$$

$$\mathfrak{T}(X; Y) = i(f_{X,Y}(\mathcal{R}_{\text{ACI}}(X; Y))) \quad (13)$$

where  $f_{X,Y}$  is an affine map defined as

$$f_{X,Y} \left( \begin{bmatrix} R_1 \\ R_2 \\ R_3 \end{bmatrix} \right) \triangleq \begin{bmatrix} R_1 \\ R_2 \\ I(X; Y) + R_1 + R_2 - R_3 \end{bmatrix}.$$

We prove (13) in Appendix B.

### A. Behavior at $R_1 = R_2 = 0$ and Connection to Gács-Körner [9]

As discussed above, Gács and Körner defined the common information,  $C_{\text{GK}}(X; Y)$  using the system in Figure 4(a), where there is no genie. Formally, an  $n$ -GK map-pair  $(g_1^{(n)}, g_2^{(n)})$  is a pair of maps  $g_1^{(n)} : \mathcal{X}^n \rightarrow \mathbb{Z}$  and  $g_2^{(n)} : \mathcal{Y}^n \rightarrow \mathbb{Z}$ . We will say that  $R_{\text{CI}}$  is an *achievable common information rate* for  $(X, Y)$  if there is a sequence of GK map-pairs  $(g_1^{(n)}, g_2^{(n)})_{n=1,2,\dots}$  such that for every  $\epsilon > 0$ , for large enough  $n$ ,

$$\Pr[g_1^{(n)}(X^n) \neq g_2^{(n)}(Y^n)] \leq \epsilon, \text{ and} \\ \frac{1}{n} H(g_1^{(n)}(X^n)) \geq R_{\text{CI}} - \epsilon.$$

GK common information  $C_{\text{GK}}(X; Y)$  is the supremum of all achievable common information rates for  $(X, Y)$ . As mentioned earlier, Gács and Körner [9] showed that  $C_{\text{GK}}(X; Y)$  is simply  $H(Q)$  where  $Q$  corresponds to the connected component in the characteristic bipartite graph of  $(X, Y)$ .

It is clear from the definition that  $(0, 0, C_{\text{GK}}(X; Y)) \in \mathcal{R}_{\text{ACI}}(X; Y)$ . However, it is not clear whether  $C_{\text{GK}}(X; Y)$  is the largest value of  $R_{\text{CI}}$  such that  $(0, 0, R_{\text{CI}}) \in \mathcal{R}_{\text{ACI}}(X; Y)$ ; i.e., if we define  $\mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y)$  as the axis intercept of the boundary of  $\mathcal{R}_{\text{ACI}}(X; Y)$  along the  $R_{\text{CI}}$  axis as follows

$$\mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y) \triangleq \max\{R_{\text{CI}} : (0, 0, R_{\text{CI}}) \in \mathcal{R}_{\text{ACI}}(X; Y)\},$$

then it is not immediately clear whether  $C_{\text{GK}}(X; Y) = \mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y)$ . This is because the absence of links from the genie is a more restrictive condition than allowing “zero-rate” links from the genie (notice the  $\epsilon$  in (8)). So we may ask whether introducing an omniscient genie, but with *zero-rate* links to the observers, changes the conclusion of Gács-Körner. In other words, whether  $\mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y)$  is larger than  $C_{\text{GK}}(X; Y)$ . The corollary below (proven in Appendix B) answers this question in the negative. Also note that the result of Gács-Körner can be obtained as a simple consequence of this corollary.

*Corollary 3.3:*

$$C_{\text{GK}}(X; Y) = \mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y) \quad (14) \\ = \max_{\substack{p_{Q|XY} \in \mathcal{P}_{X,Y}: \\ H(Q|X)=H(Q|Y)=0}} H(Q). \quad (15)$$

Further,

$$T_3^{\text{int}}(X; Y) = I(X; Y) - C_{\text{GK}}(X; Y) \quad (16)$$

Thus, at zero rates for the links, assisted common information exhibits the same trivial behavior as  $C_{\text{GK}}$ .

### B. Proof of Theorem 3.1

We first prove the converse (i.e., L.H.S.  $\subseteq$  R.H.S.). Let  $\epsilon > 0$ , and  $n$  and an  $(N_1(n), N_2(n), n)$  ACI code  $(f_1^{(n)}, f_2^{(n)}, g_1^{(n)}, g_2^{(n)})$  be such that (8)-(10) hold. Let  $C_k = f_k^{(n)}(X^n, Y^n)$ , for  $k = 1, 2$ , and  $W_1 = g_1^{(n)}(X^n, C_1)$  and  $W_2 = g_2^{(n)}(Y^n, C_2)$ . Then,

$$\begin{aligned} R_1 + \epsilon &\geq \frac{1}{n} H(C_1) \geq \frac{1}{n} H(C_1|X^n) \geq \frac{1}{n} H(W_1|X^n) \\ &\geq \frac{1}{n} I(Y^n; W_1|X^n) \\ &\stackrel{(a)}{=} \frac{1}{n} \sum_{i=1}^n H(Y_i|X_i) - H(Y_i|Y^{i-1}, X^n, W_1) \\ &\geq \frac{1}{n} \sum_{i=1}^n H(Y_i|X_i) - H(Y_i|X_i, W_1, Y^{i-1}, X^{i-1}) \\ &= \sum_{i=1}^n \frac{1}{n} I(Y_i; Q_i|X_i), \\ &\quad \text{where } Q_i \triangleq (W_1, Y^{i-1}, X^{i-1}) \\ &\stackrel{(b)}{=} I(Y_J; Q_J|X_J, J), \\ &\quad \text{where } p_J(i) \triangleq \frac{1}{n}, i \in \{1, \dots, n\}, \\ &\stackrel{(c)}{=} I(Y_J; Q|X_J), \quad \text{where } Q \triangleq (Q_J, J), \end{aligned}$$

where (a) follows from the independence of  $(X_i, Y_i)$  pairs across  $i$ . In (b), we define  $J$  to be a random variable uniformly distributed over  $\{1, \dots, n\}$  and independent of  $(X^n, Y^n)$ . And (c) follows from the independence of  $J$  and  $(X^n, Y^n)$ . Similarly,

$$\begin{aligned} R_2 + \epsilon &\geq \frac{1}{n} H(C_2|Y^n) \geq \frac{1}{n} H(W_2|Y^n) \\ &= \frac{1}{n} H(W_1, W_2|Y^n) - \frac{1}{n} H(W_1|W_2, Y^n) \\ &\geq \frac{1}{n} H(W_1|Y^n) - \frac{1}{n} H(W_1|W_2) \\ &\stackrel{(a)}{\geq} H(W_1|Y^n) - \kappa\epsilon \\ &\geq \frac{1}{n} I(X^n; W_1|Y^n) - \kappa\epsilon \\ &\stackrel{(b)}{\geq} I(X_J; Q|Y_J) - \kappa\epsilon, \end{aligned} \quad (17)$$

where (a) (with  $\kappa \triangleq 1 + \log |\mathcal{X}||\mathcal{Y}|$ ) follows from Fano's inequality and the fact that the range of  $g_1$  can be restricted without loss of generality to a set of cardinality  $|\mathcal{X}|^n |\mathcal{Y}|^n$ . And (b) can be shown along the same lines as the chain of inequalities which gave a lower bound for



$R_1$  above. Moreover,

$$\begin{aligned} \frac{1}{n} I(X^n; Y^n | W_1) &= \frac{1}{n} \sum_{i=1}^n I(X_i; Y^n | W_1, X^{i-1}) \\ &\geq \frac{1}{n} \sum_{i=1}^n I(X_i; Y_i | W_1, X^{i-1}, Y^{i-1}) \\ &= I(X_J; Y_J | Q). \end{aligned}$$

Since  $X_J, Y_J$  has the same joint distribution as  $X, Y$ , the converse for assisted residual information follows. Similarly, the converse for assisted common information can be shown using

$$\begin{aligned} \frac{1}{n} H(W_1) &\stackrel{(a)}{=} \frac{1}{n} I(X^n, Y^n; W_1) \\ &= \frac{1}{n} \sum_{i=1}^n H(X_i, Y_i) - H(X_i, Y_i | W_1, X^{i-1}, Y^{i-1}) \\ &= \frac{1}{n} \sum_{i=1}^n I(X_i, Y_i; Q_i) = I(X_J, Y_J; Q), \end{aligned}$$

where (a) follows from the fact that  $W_1$  is a deterministic function of  $(X^n, Y^n)$ . The fact that instead of  $p_{Q|XY} \in \mathcal{P}_{X,Y}$  we can consider  $p_{Q|XY} \in \hat{\mathcal{P}}_{X,Y}$  with alphabet  $\mathcal{Q}$  such that  $|\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}| + 2$  follows from Fenchel-Eggleston's strengthening of Carathéodory's theorem [6, pg. 310].

To prove achievability (i.e., L.H.S.  $\geq$  R.H.S.), we will use a result from lossy source coding. See, e.g., [4, Chapter 10] for a description of the lossy source coding problem. Consider a source  $p_S$ , and source and reconstruction alphabets  $\mathcal{S}$  and  $\hat{\mathcal{S}}$ , respectively. We have the following lemma:

**Lemma 3.4:** Given a conditional distribution  $p_{\hat{\mathcal{S}}|S}^*$ , there is a distortion measure  $d : \mathcal{S} \times \hat{\mathcal{S}} \rightarrow \mathbb{R}_+ \cup \{\infty\}$ , and a distortion constraint  $D$  such that the  $p_{\hat{\mathcal{S}}|S}^*$  is a minimizer for

$$R(D) = \min_{p_{\hat{\mathcal{S}}|S} : \mathbb{E}_{p_S p_{\hat{\mathcal{S}}|S}}[d(S, \hat{S})] \leq D} I(S; \hat{S}).$$

Moreover, unless  $I(S; \hat{S}) = 0$  (in which case any  $d$  works), the distortion measure  $d$  is given by

$$d(s, \hat{s}) = -c \log p_{\hat{\mathcal{S}}|S}^*(\hat{s}|s) + d_0(s), \quad (18)$$

where  $c > 0$  and the function  $d_0$  can be chosen arbitrarily, and

$$p_{\hat{\mathcal{S}}|S}^*(s|\hat{s}) = \frac{p_S(s) p_{\hat{\mathcal{S}}|S}^*(\hat{s}|s)}{\sum_{\tilde{s}} p_S(\tilde{s}) p_{\hat{\mathcal{S}}|S}^*(\hat{s}|\tilde{s})}.$$

The distortion constraint  $D$  is given by

$$D = \mathbb{E}_{p_S p_{\hat{\mathcal{S}}|S}^*} [d(S, \hat{S})].$$

*Proof:* See [6, Problem 3, pg. 147]; also see [10, Lemma 4] for a proof. ■

For a given  $p_{Q|XY}^* \in \hat{\mathcal{P}}_{X,Y}$ , we need to argue that

$$\begin{aligned} (I(Y; Q|X), I(X; Q|Y), I(X, Y; Q)) &\in \mathcal{R}_{\text{ACI}}(X; Y), \\ (I(Y; Q|X), I(X; Q|Y), I(X; Y|Q)) &\in \mathcal{R}_{\text{ARI}}(X; Y), \end{aligned}$$

where the conditional mutual information quantities are evaluated using the joint distribution  $p_{X,Y} p_{Q|XY}^*$ . Note that these quantities are continuous in  $p_{Q|XY}^*$ . Moreover, as was mentioned earlier, it is easy to verify from their definitions that  $\mathcal{R}_{\text{ACI}}(X; Y)$  and  $\mathcal{R}_{\text{ARI}}(X; Y)$  are closed sets. Hence, we may make the following assumption on  $p_{Q|XY}^*$  without loss of generality:

**Assumption:**  $p_{Q|XY}^*(q|x, y) > 0$  for all  $(x, y, q) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Q}$ .

In Lemma 3.4, let  $p_S$  be  $p_{X,Y}$  and  $p_{\hat{\mathcal{S}}|S}^*$  be  $p_{Q|XY}^*$ . Let  $d : \mathcal{X} \times \mathcal{Y} \times \mathcal{Q} \rightarrow \mathbb{R}_+ \cup \{\infty\}$  denote the distortion measure and  $D^*$  the distortion constraint promised by the lemma.

$$D^* = \mathbb{E}_{p_{X,Y} p_{Q|XY}^*} [d(X, Y, Q)]. \quad (19)$$

Let

$$d_{\max} = \max_{\substack{(x,y) \in \mathcal{X} \times \mathcal{Y} \\ p_{X,Y}(x,y) > 0}} \max_{q \in \mathcal{Q}} d(x, y, q).$$

Under the above Assumption, it is clear from (18) that  $d_{\max} < \infty$ .

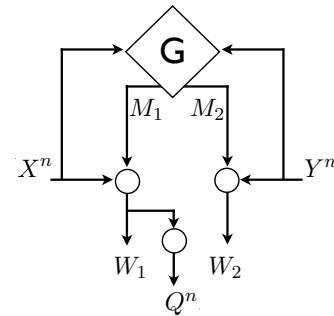


Fig. 5: Set up in the proof of Theorem 3.1

The rest of the proof proceeds as follows: we will define a distributed source coding problem (see Figure 5) where the first goal is for the observers to agree on a common random variable as in the assisted common information setup. However, instead of this common random variable meeting (10) or (11), we will require that an output sequence  $Q^n$ , which is produced as a deterministic function of the common random variable,

must meet a distortion criterion. The distortion measure and the distortion constraint are those obtained above using Lemma 3.4. We will show that these requirements can be met using a code which operates at  $(R_1, R_2) = (I(Y; Q|X), I(X; Q|Y))$ . We will then argue that this must imply that the common random variable also meets (10) and (11).

We make the following definitions (see Figure 5): we define an  $(N, N_1, N_2, n)$  code as a quintuple  $(f_1^{(n)}, f_2^{(n)}, g_1^{(n)}, g_2^{(n)}, h)$ , where

$$\begin{aligned} f_k^{(n)} : \mathcal{X}^n \times \mathcal{Y}^n &\rightarrow \{1, \dots, N_k\}, \quad k = 1, 2 \\ g_1^{(n)} : \mathcal{X}^n \times \{1, \dots, N_1\} &\rightarrow \{1, \dots, N\}, \\ g_2^{(n)} : \mathcal{Y}^n \times \{1, \dots, N_2\} &\rightarrow \{1, \dots, N\}, \text{ and} \\ h^{(n)} : \{1, \dots, N\} &\rightarrow \mathcal{Q}^n \end{aligned}$$

are deterministic functions. Note that embedded in this code is an  $(N_1, N_2, n)$  ACI code. The *probability of error* of a code is defined as

$$P_e^{(n)} = \Pr[g_1^{(n)}(X^n, f_1^{(n)}(X^n, Y^n)) \neq g_2^{(n)}(Y^n, f_2^{(n)}(X^n, Y^n))]. \quad (20)$$

Let

$$Q^n = h^{(n)}\left(g_1^{(n)}\left(X^n, f_1^{(n)}(X^n, Y^n)\right)\right).$$

For  $D \geq 0$ , we will say that  $(R_1, R_2, D)$  is *achievable* if there is a sequence of  $(N(n), N_1(n), N_2(n), n)$  codes such that for every  $\epsilon > 0$ , for sufficiently large  $n$ ,

$$\frac{1}{n} \log N_k(n) \leq R_k + \epsilon, \quad k = 1, 2 \quad (21)$$

$$P_e^{(n)} \leq \epsilon, \quad (22)$$

and the following average distortion constraint holds

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E}[d(X_i, Y_i, Q_i)] \leq D + \epsilon. \quad (23)$$

The *rate-distortion tradeoff region*  $\mathcal{R}$  is the closure of the set of all achievable  $(R_1, R_2, D)$ .

The following lemma is proved in Appendix B using standard techniques from distributed source coding theory (see, for instance, [8, Chapter 11]).

*Lemma 3.5:*

$$(I(Y; Q|X), I(X; Q|Y), D^*) \in \mathcal{R},$$

where the conditional mutual informations are evaluated using  $p_{X,Y}p_{Q|XY}^*$  and  $D^*$  is given by (19).

As mentioned above, every code has an ACI code embedded in it. We will show below that if a code satisfies (23) with  $D = D^*$  of (19), then it must

satisfy condition (10) on common information rate. More precisely,

*Claim 1:* If a sequence of  $(N(n), N_1(n), N_2(n), n)$  codes satisfy (23) with  $D = D^*$ , then it must hold that for sufficiently large  $n$ ,

$$\frac{1}{n} H(g_1^{(n)}(X^n, f_1^{(n)}(X^n, Y^n))) \geq I(X, Y; Q) - \delta(\epsilon),$$

where  $\delta(\epsilon) \downarrow 0$  as  $\epsilon \downarrow 0$  and the mutual information expression on the right-hand-side is evaluated using the joint distribution  $p_{X,Y}p_{Q|XY}^*$ .

*Proof of Claim 1:* Suppose (23) holds with  $D = D^*$ . Let  $W_1 = g_1^{(n)}(X^n, f_1^{(n)}(X^n, Y^n))$ . Then,

$$\begin{aligned} H(W_1) &\geq I(W_1; X^n Y^n) \\ &\stackrel{(a)}{\geq} I(Q^n; X^n Y^n) \\ &= \sum_{i=1}^n I(Q^n; X_i Y_i | X^{i-1} Y^{i-1}) \\ &= \sum_{i=1}^n I(Q^n X^{i-1} Y^{i-1}; X_i Y_i) \\ &\geq \sum_{i=1}^n I(Q_i; X_i Y_i), \end{aligned} \quad (24)$$

where (a) is a data processing inequality. Before we proceed further, we state some simple properties of the rate-distortion function from lossy source coding:

$$R(D) = \min_{p_{Q|XY} : \mathbb{E}[d(X, Y, Q)] \leq D} I(Q; X, Y).$$

$R(D)$  is a continuous, convex, and non-increasing function of  $D$ . A proof can be found, for instance, in [4]. Let

$$D_i = \mathbb{E}[d(X_i, Y_i, Q_i)].$$

Then

$$R(D_i) \leq I(Q_i; X_i Y_i).$$

Substituting in (24),

$$\begin{aligned} H(W_1) &\geq \sum_{i=1}^n R(D_i) \\ &\stackrel{(a)}{\geq} nR\left(\frac{1}{n} \sum_{i=1}^n D_i\right) \\ &\stackrel{(b)}{\geq} n(R(D^*) - \delta(\epsilon)), \end{aligned} \quad (25)$$

where  $\delta(\epsilon) \downarrow 0$  as  $\epsilon \downarrow 0$ . (a) is Jensen's inequality, and (b) follows from the fact that the code satisfies (23) with  $D = D^*$  and  $R(D)$  is a continuous and non-increasing function of  $D$ .

Let us recall that  $d$  and  $D^*$  were provided by Lemma 3.4 which guarantees that

$$R(D^*) = I(X, Y; Q),$$

where the mutual information is evaluated using the joint distribution  $p_{X,Y}p_{Q|XY}^*$ . Substituting this into (25) and dividing by  $n$ , we get Claim 1. ■

Further, the conditions (21)-(22) on the rates and probability of error of a sequence of codes are identical to the conditions (8)-(9) for a valid ACI strategy. Hence, we may conclude from Lemma 3.5 that

$$(I(Y; Q|X), I(X; Q|Y), I(X, Y; Q)) \in \mathcal{R}_{\text{ACI}}(X; Y).$$

To see this, for any  $\epsilon' > 0$ , notice that we may choose a small enough  $\epsilon > 0$  such that  $\epsilon' \geq \min(\epsilon, \delta(\epsilon))$ . Lemma 3.5 promises us an  $(N(n), N_1(n), N_2(n), n)$  code such that (21)-(23) are met. This implies that (8)-(9) are met with  $\epsilon'$ . Moreover, Claim 1 implies that (10) is also met with  $\epsilon'$ . This completes the characterization of  $\mathcal{R}_{\text{ACI}}(X; Y)$ .

To complete the characterization of  $\mathcal{R}_{\text{ARI}}(X; Y)$ , for  $\epsilon' > 0$ , let  $\epsilon > 0$  be chosen small enough such that  $\epsilon' \geq (3 + \log |\mathcal{X}||\mathcal{Y}|)\epsilon + \delta(\epsilon)$ . Let us consider the  $(N(n), N_1(n), N_2(n), n)$  code promised by Lemma 3.5 which satisfies (21)-(23) with  $R_1 = I(Y; Q|X)$ ,  $R_2 = I(X; Q|Y)$ , and  $D = D^*$ . Let  $W_1 = g_1^{(n)}(X^n, f_1^{(n)}(X^n, Y^n))$ . We have the following information theoretic identity (see (52) on page 21):

$$\begin{aligned} I(X^n; Y^n | W_1) &= I(X^n; Y^n) + I(X^n; W_1 | Y^n) \\ &\quad + I(Y^n; W_1 | X^n) - I(X^n Y^n; W_1). \end{aligned} \quad (26)$$

But,

$$\begin{aligned} I(Y^n; W_1 | X^n) &= I(Y^n; g_1^{(n)}(X^n, f_1^{(n)}(X^n, Y^n)) | X^n) \\ &\leq I(Y^n; f_1^{(n)}(X^n, Y^n) | X^n) \\ &\leq \log N_1(n). \end{aligned} \quad (27)$$

Using (22) and following the same argument which lead us to (17), we can write

$$I(X^n; W_1 | Y^n) \leq \log N_2(n) + n\kappa\epsilon, \quad (28)$$

where  $\kappa \triangleq 1 + \log |\mathcal{X}||\mathcal{Y}|$ . Further, by Claim 1,

$$\begin{aligned} I(X^n Y^n; W_1) &= H(W_1) \\ &\geq n(I(X, Y; Q) - \delta(\epsilon)). \end{aligned} \quad (29)$$

Substituting the above three in (26) and using (21) with  $R_1 = I(Y; Q|X)$  and  $R_2 = I(X; Q|Y)$ ,

$$\begin{aligned} \frac{1}{n} I(X^n; Y^n | W_1) &\leq I(X; Y) + I(Y; Q|X) + I(X; Q|Y) \\ &\quad - I(X, Y; Q) + (\kappa + 2)\epsilon + \delta(\epsilon) \\ &= I(X; Y|Q) + \epsilon', \end{aligned} \quad (30)$$

where the last equality is again (52). Hence, we may conclude that

$$(I(Y; Q|X), I(X; Q|Y), I(X; Y|Q)) \in \mathcal{R}_{\text{ARI}}(X; Y).$$

This completes the characterization of  $\mathcal{R}_{\text{ARI}}$ .

#### IV. THE GRAY-WYNER SYSTEM AND ITS RELATIONSHIP TO REGION OF TENSION AND ASSISTED COMMON INFORMATION

##### A. Gray-Wyner system

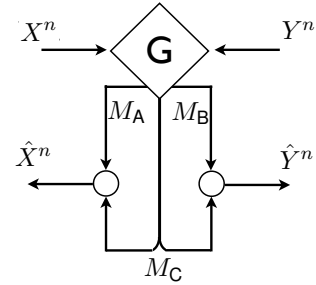


Fig. 6: Setup for Gray-Wyner (GW) system.

The Gray-Wyner system is shown in Figure 6. It is a source coding problem where an encoder who observes the pair of correlated sources  $X^n, Y^n$  maps it to three messages: two “private” messages  $M_A = f_A^{(n)}(X^n, Y^n)$ ,  $M_B = f_B^{(n)}(X^n, Y^n)$ , and a “common” message  $M_C = f_C^{(n)}(X^n, Y^n)$ . There are two decoders which attempt to recover  $X^n$  and  $Y^n$  respectively. The first decoder tries to estimate  $X^n$  using the private message  $M_A$  and the common message  $M_C$  as  $\hat{X}^n = g_{AC}^{(n)}(M_A, M_C)$ , and the second decoder tries to estimate  $Y^n$  from  $M_B, M_C$  as  $\hat{Y}^n = g_{BC}^{(n)}(M_B, M_C)$ . Gray-Wyner problem is to characterize the rates of the messages so that the decoders estimate losslessly.

More precisely, for a pair of random variables  $(X, Y)$ , an  $(N_A, N_B, N_C, n)$  GW code  $(f_A^{(n)}, f_B^{(n)}, f_C^{(n)}, g_{AC}^{(n)}, g_{BC}^{(n)})$ , is such that

$$\begin{aligned} f_\alpha^{(n)} : \mathcal{X}^n \times \mathcal{Y}^n &\rightarrow \{1, \dots, N_\alpha\}, \text{ where } \alpha = A, B, C, \\ g_{AC}^{(n)} : \{1, \dots, N_A\} \times \{1, \dots, N_C\} &\rightarrow \mathcal{X}^n, \text{ and} \\ g_{BC}^{(n)} : \{1, \dots, N_B\} \times \{1, \dots, N_C\} &\rightarrow \mathcal{Y}^n \end{aligned}$$

are deterministic functions. We say that  $(R_A, R_B, R_C)$  is *achievable in the Gray-Wyner system* for  $(X, Y)$ , if there is a sequence of  $(N_A(n), N_B(n), N_C(n), n)$  GW codes  $(f_A^{(n)}, f_B^{(n)}, f_C^{(n)}, g_{AC}^{(n)}, g_{BC}^{(n)})$  such that for every  $\epsilon > 0$ ,

for large enough  $n$

$$\begin{aligned} \frac{1}{n} \log N_\alpha(n) &\leq R_\alpha + \epsilon, \quad \alpha = \mathbf{A}, \mathbf{B}, \mathbf{C}, \\ \Pr[g_{\mathbf{AC}}^{(n)}(f_{\mathbf{A}}^{(n)}(X^n, Y^n), f_{\mathbf{C}}^{(n)}(X^n, Y^n)) \neq X^n] &\leq \epsilon, \\ \Pr[g_{\mathbf{BC}}^{(n)}(f_{\mathbf{B}}^{(n)}(X^n, Y^n), f_{\mathbf{C}}^{(n)}(X^n, Y^n)) \neq Y^n] &\leq \epsilon. \end{aligned}$$

**Definition 4.1:** The Gray-Wyner region  $\mathcal{R}_{\text{GW}}(X; Y)$  is the closure of the set of all rate 3-tuples that are achievable in the Gray-Wyner system for  $(X, Y)$ .

We write  $\mathcal{R}_{\text{GW}}$  when the random variables are clear from the context.

A simple bound on  $\mathcal{R}_{\text{GW}}(X; Y)$  is given by  $\mathcal{R}_{\text{GW}}(X; Y) \subseteq \mathcal{L}_{\text{GW}}(X; Y)$ , where

$$\mathcal{L}_{\text{GW}}(X; Y) \triangleq \{(R_A, R_B, R_C) : R_A + R_C \geq H(X), R_B + R_C \geq H(Y), R_A + R_B + R_C \geq H(X, Y)\} \quad (31)$$

The Gray-Wyner region was characterized in [11].

**Theorem 4.1 ([11]):**  $\mathcal{R}_{\text{GW}}(X; Y)$  equals

$$i\left(\{(H(X|Q), H(Y|Q), I(X, Y; Q)) : p_{Q|XY} \in \hat{\mathcal{P}}_{X,Y}\}\right).$$

Wyner's common information [31],  $C_{\text{Wyner}}(X; Y)$  of a pair of random variables  $X, Y$  is defined in terms of the Gray-Wyner system. It is the smallest  $R_C$  such that the outputs of the encoder taken together is an asymptotically efficient representation of  $(X, Y)$ , i.e., when  $R_A + R_B + R_C = H(X, Y)$ . Using the above theorem we have

**Theorem 4.2 ([31]):**

$$\begin{aligned} C_{\text{Wyner}}(X; Y) &\triangleq \inf_{\substack{(R_A, R_B, R_C) \in \mathcal{R}_{\text{GW}}(X; Y), \\ R_A + R_B + R_C = H(X, Y)}} R_C \\ &= \min_{\substack{p_{Q|XY} \in \mathcal{P}_{X,Y}: \\ X-Q-Y}} I(X, Y; Q) \end{aligned}$$

It is known that Gács-Körner common information can be obtained from the Gray-Wyner region [6, Problem 4.28, pg. 404].

$$C_{\text{GK}}(X; Y) = \max_{\substack{R_A + R_C = H(X), R_B + R_C = H(Y), \\ (R_A, R_B, R_C) \in \mathcal{R}_{\text{GW}}}} R_C \quad (32)$$

Alternatively [17],

$$C_{\text{GK}}(X; Y) = \max_{\substack{R \leq I(X; Y), \\ \{R_C = R\} \cap \mathcal{L}_{\text{GW}} \subseteq \mathcal{R}_{\text{GW}}}} R \quad (33)$$

## B. New Connections

Analogous to Corollary 3.2, the following theorem (proved in the appendix) shows that the region of tension of  $(X, Y)$  can be expressed in terms of their Gray-Wyner region.

**Theorem 4.3:**

$$\mathfrak{T}(X; Y) = i(g_{X,Y}(\mathcal{R}_{\text{GW}}(X; Y))),$$

where  $g_{X,Y}$  is an affine map defined as

$$g_{X,Y} \left( \begin{bmatrix} R_A \\ R_B \\ R_C \end{bmatrix} \right) \triangleq \begin{bmatrix} R_A + R_C - H(X) \\ R_B + R_C - H(Y) \\ R_A + R_B + R_C - H(X, Y) \end{bmatrix}.$$

Thus, the tension region  $\mathfrak{T}(X; Y)$  is the increasing hull of the Gray-Wyner region  $\mathcal{R}_{\text{GW}}(X; Y)$  under an affine map  $g_{X,Y}$ . The map, in fact, computes the gap of  $\mathcal{R}_{\text{GW}}(X; Y)$  to the simple lower bound  $\mathcal{L}_{\text{GW}}(X; Y)$  of (31). The first coordinate of  $\mathcal{R}'_{\text{GW}}$  is the gap between the (sum) rate at which the first decoder in the Gray-Wyner system receives data and the minimum possible rate at which it may receive data so that it can losslessly reproduce  $X^n$ . The second coordinate has a similar interpretation with respect to the second decoder. The third coordinate is the gap between the rate at which the encoder sends data and the minimum possible rate at which it may transmit to allow both decoders to losslessly reproduce their respective sources.

Though Theorem 4.3 shows that the region of tension is closely related to the Gray-Wyner region, it must be noted that the latter does not possess an essential monotonicity property of the region of tension that is discussed in Section V, and is therefore less-suited for the cryptographic application which motivates this paper.

The relations (32) and (33) fall out of Theorem 4.3 and Corollary 3.3.

**Corollary 4.4:**

$$C_{\text{GK}}(X; Y) = \max_{\substack{R_A + R_C = H(X), R_B + R_C = H(Y), \\ (R_A, R_B, R_C) \in \mathcal{R}_{\text{GW}}}} R_C \quad (32)$$

$$C_{\text{GK}}(X; Y) = \max_{\substack{R \leq I(X; Y), \\ \{R_C = R\} \cap \mathcal{L}_{\text{GW}} \subseteq \mathcal{R}_{\text{GW}}}} R \quad (33)$$

Another consequence of Theorem 4.3 is an expression for Wyner's common information  $C_{\text{Wyner}}(X; Y)$  in terms of  $\mathfrak{T}(X; Y)$  (see Figure 1):

**Corollary 4.5:**

$$C_{\text{Wyner}}(X; Y) = I(X; Y) + \min_{(R_1, R_2, 0) \in \mathfrak{T}(X; Y)} R_1 + R_2. \quad (34)$$

As we have seen already, one of the axes intercepts of  $\mathfrak{T}(X; Y)$ , namely  $T_3^{\text{int}}(X; Y)$  is closely connected to the GK common information ( $C_{\text{GK}}(X; Y) = I(X; Y) - T_3^{\text{int}}(X; Y)$ ). The other two axes intercepts also turn out to be closely connected to certain quantities identified elsewhere in the context of source coding [20], [17]. Before we look at this connection, let us reinterpret these two axes intercepts using the fact that  $\mathfrak{T}(X; Y) = \mathcal{R}_{\text{ARI}}(X; Y)$  (Corollary 3.2).

In the context of the assisted common information system in Figure 4(b),  $T_1^{\text{int}}(X; Y)$  (resp.,  $T_2^{\text{int}}(X; Y)$ ) is the rate at which the genie must communicate when it has a link to only the user who receives  $X$  (resp.  $Y$ ) source so that the users can produce a common random variable conditioned on which the sources are independent<sup>7</sup>. We have already seen in Theorem 2.2 that

$$T_1^{\text{int}}(X; Y) = \min_{\substack{p_{Q|XY} \in \mathcal{P}_{X,Y}: \\ I(X; Q|Y) = I(X; Y|Q) = 0}} I(Y; Q|X), \quad (35)$$

$$T_2^{\text{int}}(X; Y) = \min_{\substack{p_{Q|XY} \in \mathcal{P}_{X,Y}: \\ I(Y; Q|X) = I(X; Y|Q) = 0}} I(X; Q|Y). \quad (36)$$

We will show below that this pair is closely related to a pair of quantities identified in the context of lossless coding with side-information [20] and the Gray-Wyner system [17]. Let (following the notation of [17])

$$\begin{aligned} G(Y \rightarrow X) &= \min\{R_C : (H(X|Y), H(Y) - R_C, R_C) \in \mathcal{R}_{\text{GW}}(X; Y)\}, \\ G(X \rightarrow Y) &= \min\{R_C : (H(X) - R_C, H(Y|X), R_C) \in \mathcal{R}_{\text{GW}}(X; Y)\}. \end{aligned}$$

It has been shown [20], [17] that  $G(Y \rightarrow X)$  is the smallest rate at which side-information  $Y$  may be coded and sent to a decoder which is interested in recovering  $X$  with asymptotically vanishing probability of error if the decoder receives  $X$  coded and sent at a rate of only  $H(X|Y)$  (which is the minimum possible rate which will allow such recovery). Further, [17] arrives at the maximum of  $G(Y \rightarrow X)$  and  $G(X \rightarrow Y)$  as a dual to the alternative definition of  $C_{\text{GK}}$  in (33) from the Gray-Wyner system.

We prove the following relationship between the two pairs of quantities in the appendix.

<sup>7</sup>Though the definition allows for zero-rate communication to the other user and a zero-rate (but non-zero) residual conditional mutual information, it can be shown from the expression for these rates in (35)-(36) that there is a scheme which achieves exact conditional independence and requires no communication to the other user. The proof is similar to that of Corollary 3.3.

*Corollary 4.6:*

$$G(Y \rightarrow X) = I(X; Y) + T_1^{\text{int}}(X; Y), \quad (37)$$

$$G(X \rightarrow Y) = I(X; Y) + T_2^{\text{int}}(X; Y). \quad (38)$$

Further,

$$\begin{aligned} \min\{R : R \geq I(X; Y), \\ (R_C = R) \cap \mathcal{L}_{\text{GW}}(X; Y) \subseteq \mathcal{R}_{\text{GW}}(X; Y)\} \\ = \max(G(Y \rightarrow X), G(X \rightarrow Y)) \quad (39) \\ = I(X; Y) + \max(R_{1-0}, R_{2-0}). \quad (40) \end{aligned}$$

## V. UPPERBOUNDS ON THE EFFICIENCY OF TWO-PARTY SECURE SAMPLING PROTOCOLS

We will now apply the concept of tension to derive upperbounds on the efficiency of two-party secure sampling protocols. A two-party protocol  $\Pi$  is specified by a pair of (possibly randomized) functions  $\pi_{\text{Alice}}$  and  $\pi_{\text{Bob}}$ , that are used by each party to operate on its current state  $W$  to produce a message  $m$  (that is sent to the other party) and a new state  $W'$  for itself. The initial state of the parties may consist of correlated random variables  $(X, Y)$ , with Alice's state being  $X$  and Bob's state being  $Y$ ; such a pair is called a *set up* for the protocol. The protocol proceeds by the parties taking turns to apply their respective functions to their state, and sending the resulting message to the other party; this message is added to the state of the other party.  $\pi_{\text{Alice}}$  and  $\pi_{\text{Bob}}$  also specify when the protocol terminates and produces output (instead of producing the next message in the protocol). A protocol is considered *valid* only if both parties terminate in a finite number of rounds (with probability 1). The *view* of a party in an execution of the protocol is a random variable which is defined as the sequence of its states so far in the protocol execution. For a valid protocol  $\Pi = (\pi_{\text{Alice}}, \pi_{\text{Bob}})$ , we shall denote the final views of the two parties as  $(\Pi_{\text{Alice}}^{\text{view}}(X; Y), \Pi_{\text{Bob}}^{\text{view}}(X; Y))$ . Also, we shall denote the outputs as  $(\Pi_{\text{Alice}}^{\text{out}}(X; Y), \Pi_{\text{Bob}}^{\text{out}}(X; Y))$ . (Later, when it is clear, we abbreviate these as  $(\Pi_{\text{Alice}}^{\text{view}}, \Pi_{\text{Bob}}^{\text{view}})$  and  $(\Pi_{\text{Alice}}^{\text{out}}, \Pi_{\text{Bob}}^{\text{out}})$  respectively.)

Now we define (perfectly) secure sampling. (Extension to statistically secure sampling, which allows a vanishing error, is treated in Section V-D.)

*Definition 5.1:* We say that a pair of correlated random variables  $(U, V)$  can be (perfectly) *securely sampled* using a pair of correlated random variables  $(X, Y)$  as set up if there exists a valid protocol  $\Pi = (\pi_{\text{Alice}}, \pi_{\text{Bob}})$  such

that

$$(\Pi_{\text{Alice}}^{\text{out}}(X; Y), \Pi_{\text{Bob}}^{\text{out}}(X; Y)) \sim p_{U,V} \quad (41)$$

$$\Pi_{\text{Alice}}^{\text{view}}(X; Y) - \Pi_{\text{Alice}}^{\text{out}}(X; Y) - \Pi_{\text{Bob}}^{\text{out}}(X; Y) \quad (42)$$

$$\Pi_{\text{Alice}}^{\text{out}}(X; Y) - \Pi_{\text{Bob}}^{\text{out}}(X; Y) - \Pi_{\text{Bob}}^{\text{view}}(X; Y) \quad (43)$$

In this case we say  $\Pi^{(X,Y)} \rightsquigarrow (U, V)$ .

The three conditions above correspond to correctness (when neither party is corrupt), security for Bob when Alice is corrupt, and security for Alice when Bob is corrupt. The correctness condition in (41) is obvious: the outputs  $(\Pi_{\text{Alice}}^{\text{out}}(X; Y), \Pi_{\text{Bob}}^{\text{out}}(X; Y))$  must be identically distributed as  $(U, V)$ . The condition in (42) says that even if Alice is “curious” (or “passively corrupt”) and retains her view in the entire protocol, it should give her no more information about Bob’s output than just her own output at the end of the protocol provides. (43) gives the symmetric condition for when Bob is curious.

#### A. Towards Measuring Cryptographic Content

As metioned in Section II, in [29] three information theoretic quantities were introduced, which we identified as the three axes intercepts of  $\mathfrak{T}(X; Y)$ . As shown in [29], these quantities are “monotones” that can only decrease in a protocol, and if the protocol securely realizes a pair of correlated random variables  $(U, V)$  using a set up  $(X, Y)$ , then each of these quantities should be at least as large for  $(X, Y)$  as for  $(U, V)$ . Thus such a monotone can be thought of as a quantitative measure of cryptographic content in the sense that  $(U, V)$  with a higher cryptographic content cannot be generated from a set up  $(X, Y)$  with a lower cryptographic content.

While the quantities in [29] do capture several interesting cryptographic properties, they paint a very incomplete picture. For instance, two pairs of correlated random variables  $(X, Y)$  and  $(X', Y')$  may have vastly different values for these quantities, even if they are statistically close to each other, and hence have similar “cryptographic content.”

Instead, we shall consider the three dimensional region  $\mathfrak{T}(X; Y)$  and show that the region as a whole satisfies a monotonicity property: the region can only expand (grow towards the origin) when  $(X, Y)$  evolve as the views of the two parties in a protocol (or outputs “securely derived” from the views in a protocol). Hence if the protocol securely realizes a pair of correlated random variables  $(U, V)$  using a set up  $(X, Y)$ , then  $\mathfrak{T}(X; Y)$  should be contained within  $\mathfrak{T}(U; V)$ . As we shall see, since the region  $\mathfrak{T}(X; Y)$  has a non-trivial shape (see for instance, Example 2.2),  $\mathfrak{T}(X; Y)$  can yield much better bounds on the rate than just considering the

axis intercepts; in particular  $\mathfrak{T}(X; Y)$  can differentiate between pairs of correlated random variables that have the same axis intercepts. Further  $\mathfrak{T}(X; Y)$  is continuous as a function of  $p_{X,Y}$ , and as such one can derive rate bounds that are applicable to statistical security as well as perfect security.

#### B. Monotone Regions for 2-Party Secure Protocols

*Definition 5.2:* We will call a function  $\mathcal{M}$  that maps a pair of random variables  $X$  and  $Y$ , to an upward closed subset<sup>8</sup> of  $\mathbb{R}_+^d$  (points in the  $d$ -dimensional real space with non-negative co-ordinates) a *monotone region* if it satisfies the following properties:

- 1) (*Local computation cannot shrink it.*) For all jointly distributed random variables  $(X, Y, Z)$  with  $X - Y - Z$ , we have  $\mathcal{M}(XY; Z) \supseteq \mathcal{M}(Y; Z)$  and  $\mathcal{M}(X; YZ) \supseteq \mathcal{M}(X; Y)$ .
- 2) (*Communication cannot shrink it.*) For all jointly distributed random variables  $(X, Y)$  and functions  $f$  (over the support of  $X$  or  $Y$ ), we have  $\mathcal{M}(X; Yf(X)) \supseteq \mathcal{M}(X; Y)$  and  $\mathcal{M}(Xf(Y); Y) \supseteq \mathcal{M}(X; Y)$ .
- 3) (*Securely derived outputs do not have smaller regions.*) For all jointly distributed random variables  $(X, U, V, Y)$  with  $X - U - V$  and  $U - V - Y$ , we have  $\mathcal{M}(U; V) \supseteq \mathcal{M}(XU; YV)$ .
- 4) (*Regions of independent pairs add up.*) For independent pairs of jointly distributed random variables  $(X_1, Y_1)$  and  $(X_2, Y_2)$ , we have  $\mathcal{M}(X_1X_2; Y_1Y_2) = \mathcal{M}(X_1; Y_1) + \mathcal{M}(X_2; Y_2)$ , where the  $+$  sign denotes *Minkowski sum*. In other words,  $\mathcal{M}(X_1X_2; Y_1Y_2) = \{\mathbf{a}_1 + \mathbf{a}_2 \mid \mathbf{a}_1 \in \mathcal{M}(X_1; Y_1) \text{ and } \mathbf{a}_2 \in \mathcal{M}(X_2; Y_2)\}$ . (Here addition denotes coordinate-wise addition.)

Note that since  $\mathcal{M}(X_1; Y_1)$  and  $\mathcal{M}(X_2; Y_2)$  have non-negative co-ordinates and are upward closed,  $\mathcal{M}(X_1; Y_1) + \mathcal{M}(X_2; Y_2)$  is smaller than both of them. This is consistent with the intuition that more cryptographic content (as would be the case with having more independent copies of the random variables) corresponds to a smaller region.

Our definition of a monotone region strictly generalizes that suggested by [29]. The monotone in [29], which is a single real number  $m$ , can be interpreted as a one-dimensional region  $[m, \infty)$  to fit our definition. (Note that a decrease in the value of  $m$  corresponds to the region  $[m, \infty)$  enlarging.)

<sup>8</sup>A subset  $\mathcal{M}$  of  $\mathbb{R}^d$  is called upward closed if  $\mathbf{a} \in \mathcal{M}$  and  $\mathbf{a}' \geq \mathbf{a}$  (i.e., each co-ordinate of  $\mathbf{a}'$  is no less than that of  $\mathbf{a}$ ) implies that  $\mathbf{a}' \in \mathcal{M}$ .

*Theorem 5.1:* If  $n_1$  independent copies of a pair of correlated random variables  $(U, V)$  can be securely realized using  $n_2$  independent copies of a pair of correlated random variables  $(X, Y)$  as set up, then for any monotone region  $\mathcal{M}$ ,  $n_2\mathcal{M}(X; Y) \subseteq n_1\mathcal{M}(U; V)$ . (Here multiplication by an integer  $n$  refers to  $n$ -times repeated Minkowski sum.)

*Proof:* Consider some protocol  $\Pi$  such that  $\Pi^{(X^{n_2}, Y^{n_2})} \rightsquigarrow (U^{n_1}, V^{n_1})$ . Let  $t$  be the maximum number of messages in the protocol. For  $i = 0, \dots, t$ , let  $(X_i, Y_i)$  denote the views of the parties after the  $i^{\text{th}}$  message. Then  $(X_0, Y_0) = (X^{n_2}, Y^{n_2})$  and  $(X_t, Y_t) = (\Pi_{\text{Alice}}^{\text{view}}, \Pi_{\text{Bob}}^{\text{view}})$ . By Condition (1) and Condition (2) of Definition 5.2,  $\mathcal{M}(X_{i+1}; Y_{i+1}) \supseteq \mathcal{M}(X_i; Y_i)$  (note that we do allow the local computation defined by  $\pi_{\text{Alice}}$  and  $\pi_{\text{Bob}}$  to be randomized, but the randomness used is independent of the other party's view). By (41)-(43) as applied to  $\Pi^{(X^{n_2}, Y^{n_2})} \rightsquigarrow (U^{n_1}, V^{n_1})$ , and Condition (3),  $\mathcal{M}(U^{n_1}; V^{n_1}) = \mathcal{M}(\Pi_{\text{Alice}}^{\text{out}}; \Pi_{\text{Bob}}^{\text{out}}) \supseteq \mathcal{M}(X_t; Y_t)$ . Thus,  $\mathcal{M}(U^{n_1}; V^{n_1}) \supseteq \mathcal{M}(X^{n_2}; Y^{n_2})$ . Finally, by Condition (4) we obtain the claimed inclusion. ■

### C. Using Tension to Bound Rate of Secure Sampling.

Theorem 5.1 gives us a means to use an appropriate monotone region to bound the *rate* of securely sampling instances of a pair  $(U, V)$  from a set up  $(X, Y)$ . We define this rate as follows (where  $(X^n, Y^n)$  denotes  $n$  independent copies of  $(X, Y)$ ).

*Definition 5.3:* For pairs of correlated random variables  $(U, V)$  and  $(X, Y)$  (i.e., p.m.f.s  $p_{UV}$  and  $p_{XY}$ ), the *rate of securely sampling  $(U, V)$  from  $(X, Y)$*  is defined as<sup>9</sup>

$$\sup\left\{\frac{n_1}{n_2} : \exists \Pi, n_1, n_2 \text{ s.t. } \Pi^{(X^{n_2}, Y^{n_2})} \rightsquigarrow (U^{n_1}, V^{n_1})\right\}.$$

Note that in Theorem 5.1,  $n$ -times repeated Minkowski sum of  $\mathcal{M}$  is

$$n\mathcal{M} = \{\mathbf{a}_1 + \dots + \mathbf{a}_n \mid \mathbf{a}_1, \dots, \mathbf{a}_n \in \mathcal{M}\}.$$

In general, the shape of the  $n$ -times Minkowski sum of a region changes with  $n$  and would make it difficult to work with. But if  $\mathcal{M}$  is convex, then this multiplication operation gives the same region as the following definition of multiplication by a real number  $r > 0$ :

$$r \cdot \mathcal{M} = \{r\mathbf{a} \mid \mathbf{a} \in \mathcal{M}\} \quad (\text{for convex } \mathcal{M}). \quad (44)$$

This gives us a convenient way to bound the rate, if we use a *convex monotone region*. The following is an immediate corollary of Theorem 5.1 (and the fact that

for convex regions  $\mathcal{M}_1$  and  $\mathcal{M}_2$ ,  $n_2\mathcal{M}_2 \subseteq n_1\mathcal{M}_1$  iff  $\mathcal{M}_2 \subseteq \frac{n_1}{n_2}\mathcal{M}_1$ ).

*Corollary 5.2:* For any convex monotone region  $\mathcal{M}$ , if the rate of securely sampling  $(U, V)$  from  $(X, Y)$  is  $r > 0$ , then  $\mathcal{M}(X; Y) \subseteq r \cdot \mathcal{M}(U; V)$ . (Here, multiplication of a region by a real number is as in (44).)

The importance of the above corollary is that the region of tension provides us with a “good” convex monotone region, which can be used to obtain state-of-the-art bounds on the rate.

*Theorem 5.3:*  $\mathfrak{T}$  is a (3-dimensional) monotone region (as in Definition 5.2).

In fact, we shall show a more general result in Theorem 5.6, which implies the above theorem. Combined with the fact that  $\mathfrak{T}$  is convex (Theorem 2.3), Theorem 5.3 and Corollary 5.2 yield the following result (which will also be generalized in Corollary 5.7).

*Corollary 5.4:* If the rate of securely sampling  $(U, V)$  from  $(X, Y)$  is  $r > 0$ , then  $\mathfrak{T}(X; Y) \subseteq r \cdot \mathfrak{T}(U; V)$ .

Note that this gives an *upperbound* on  $r$ , because, as  $r$  increases from 0, the region  $r \cdot \mathfrak{T}(X; Y)$  shrinks away from the origin.

In general, we can obtain tighter bounds this way than yielded by the three monotones considered in [29] (namely, the axis intercepts of this monotone region), because the region of tension can “bulge” towards the origin. In other words, the intercepts, and in particular the common information of Gács and Körner, do not by themselves capture subtle characteristics of correlation that are reflected in *the shape of the monotone region*. Below, we give a concrete example where the region of tension does give us a tighter bound than the monotones of [29].

*Example 5.1:* Consider the question of securely realizing  $n_1$  independent pairs of random variables distributed according to  $(U, V)$  in Example 2.2 from  $n_2$  independent pairs of  $(X, Y)$  in Example 2.1. While the monotones in [29] will give an upperbound of 1.930 on the rate  $n_1/n_2$ , we show that  $n_1/n_2 \leq 0.551$ . (For this we use the intersection of  $\mathfrak{T}(U; V)$  with the plane  $z = 0$  (Figure 3) and one point in the region  $\mathfrak{T}(X; Y)$  (marked in Figure 2); then by Corollary 5.4,  $0.1143 \geq 0.2075 \cdot r$ . Note that we do not claim this is the tightest bound we can obtain from Corollary 5.4: we do not check if  $\mathfrak{T}(X; Y) \subseteq r \cdot \mathfrak{T}(U; V)$  for this value of  $r$ , since we do not compute the entire boundary of the two three-dimensional regions.)

<sup>9</sup>Here we let  $\frac{n_1}{n_2} = 0$  when  $n_1 = n_2 = 0$ .

### D. Statistical Security

Recall that the security conditions ((41)–(43)) for a protocol  $\Pi$  sampling  $(U, V)$  from a set up  $(X, Y)$  relate  $\Pi_{\text{Alice}}^{\text{out}}(X; Y)$ ,  $\Pi_{\text{Bob}}^{\text{out}}(X; Y)$ ,  $\Pi_{\text{Alice}}^{\text{view}}(X; Y)$ ,  $\Pi_{\text{Bob}}^{\text{view}}(X; Y)$  with  $U, V$  and with each other. These conditions are for *perfect security*. A more realistic notion of security allows a small error in all these three conditions. Such a notion is referred to as *statistical security*. Below, we present a standard “simulation-based” definition of statistical security. (Below, we will abbreviate  $\Pi_{\text{Alice}}^{\text{out}}(X; Y)$ ,  $\Pi_{\text{Alice}}^{\text{view}}(X; Y)$  etc. by  $\Pi_{\text{Alice}}^{\text{out}}$ ,  $\Pi_{\text{Alice}}^{\text{view}}$  etc., for the sake of readability.)

**Definition 5.4:** For  $\epsilon \geq 0$ , a protocol  $\Pi$  is said to  $\epsilon$ -securely sample a pair of correlated random variables  $(U, V)$  using a pair of correlated random variables  $(X, Y)$  as set up if there exists a valid protocol  $\Pi = (\pi_{\text{Alice}}, \pi_{\text{Bob}})$  and random variables (“simulated views”)  $\Sigma_{\text{Alice}}^{\text{view}}$  and  $\Sigma_{\text{Bob}}^{\text{view}}$ , over the alphabets of  $\Pi_{\text{Alice}}^{\text{view}}$  and  $\Pi_{\text{Bob}}^{\text{view}}$  respectively, distributed according to  $p_{\Sigma_{\text{Alice}}^{\text{view}}|U, V}$  and  $p_{\Sigma_{\text{Bob}}^{\text{view}}|U, V}$  such that

$$\Sigma_{\text{Alice}}^{\text{view}} - U - V \quad \text{and} \quad U - V - \Sigma_{\text{Bob}}^{\text{view}} \quad (45)$$

$$\Delta((U, V), (\Pi_{\text{Alice}}^{\text{out}}, \Pi_{\text{Bob}}^{\text{out}})) \leq \epsilon \quad (46)$$

$$\Delta((\Sigma_{\text{Alice}}^{\text{view}}, V), (\Pi_{\text{Alice}}^{\text{view}}, \Pi_{\text{Bob}}^{\text{out}})) \leq \epsilon \quad (47)$$

$$\Delta((U, \Sigma_{\text{Bob}}^{\text{view}}), (\Pi_{\text{Alice}}^{\text{out}}, \Pi_{\text{Bob}}^{\text{view}})) \leq \epsilon \quad (48)$$

Here  $\Delta(\cdot, \cdot)$  stands for the total variation distance. In this case we say  $\Pi^{(X, Y)} \xrightarrow{\epsilon} (U, V)$ .

**Remark:**  $\Pi^{(X, Y)} \xrightarrow{0} (U, V)$  if and only if  $\Pi^{(X, Y)} \rightsquigarrow (U, V)$  (Definition 5.1). In particular, it can be shown that if  $\Pi^{(X, Y)} \xrightarrow{0} (U, V)$ , then (42) and (43) hold (see for instance, Lemma D.1). In the other direction, if  $\Pi^{(X, Y)} \rightsquigarrow (U, V)$ , then one can take  $p_{\Sigma_{\text{Alice}}^{\text{view}}|U, V} = p_{\Pi_{\text{Alice}}^{\text{view}}|\Pi_{\text{Alice}}^{\text{out}}, \Pi_{\text{Bob}}^{\text{out}}}$  and  $p_{\Sigma_{\text{Bob}}^{\text{view}}|U, V} = p_{\Pi_{\text{Bob}}^{\text{view}}|\Pi_{\text{Alice}}^{\text{out}}, \Pi_{\text{Bob}}^{\text{out}}}$ .

**Definition 5.5:** We say  $(U, V)$  can be *statistically securely sampled* using a pair of correlated random variables  $(X, Y)$  as set up if, for any  $\epsilon > 0$ , there is a valid protocol  $\Pi$  and positive integers  $n_1, n_2$  such that  $\Pi^{(X^{n_2}, Y^{n_2})} \xrightarrow{\epsilon} (U^{n_1}, V^{n_1})$ . Then, the *rate of statistically securely sampling*  $(U, V)$  from  $(X, Y)$  is defined as

$$\limsup_{\epsilon \downarrow 0} \left\{ \frac{n_1}{n_2} : \exists \Pi, n_1, n_2 \text{ s.t. } \Pi^{(X^{n_2}, Y^{n_2})} \xrightarrow{\epsilon} (U^{n_1}, V^{n_1}) \right\}$$

**Remark:** The typical definition of security in cryptography literature requires the protocol  $\Pi$  to be *uniform* (i.e., the protocol for all values of  $\epsilon$  can be implemented by a single Turing Machine that takes  $\epsilon$  as input) and also “efficient” (i.e., the Turing Machine implementing the protocol runs in time (say) polynomial in  $\log 1/\epsilon$ ). Since we shall be proving negative results, using the

weaker security definitions without these restrictions only strengthens our results.

**Robust Monotone Regions:** We generalize the definition of a monotone region (Definition 5.2) by strengthening item (3) in the definition to the following conditions, to obtain the definition of a “robust monotone region.”

**Definition 5.6:** We will call a function  $\mathcal{M}$  that maps a pair of random variables  $X$  and  $Y$ , to an upward closed subset of  $\mathbb{R}_+^d$  a *robust-monotone region* if it is a monotone region (as in Definition 5.2), and the following hold:

3') (Statistically securely derived outputs do not have a much smaller region.) There exists a constant  $c \geq 0$  such that, for any jointly distributed random variables  $(X, U, V, Y)$  and  $\phi \geq 0$ , if  $I(X; V|U) \leq \phi$  and  $I(U; Y|V) \leq \phi$ , then

$$\mathcal{M}(U; V) \supseteq \mathcal{M}(XU; YV) + c\phi.$$

3'') (Continuity, Convexity and Closure.) There exists a bounded, continuous function  $\hat{\delta} : [0, 1] \rightarrow \mathbb{R}_+$  with  $\hat{\delta}(0) = 0$ , such that for any two pairs of correlated random variables  $(X, Y)$  and  $(X', Y')$ , both over alphabet  $\mathcal{X} \times \mathcal{Y}$ , and  $\epsilon \in [0, 1]$ , if  $\Delta(XY, X'Y') = \epsilon$ , then  $\mathcal{M}(X; Y) \subseteq \mathcal{M}(X'; Y') - \hat{\delta}(\epsilon) \cdot \log |\mathcal{X}| |\mathcal{Y}|$ . Also,  $\mathcal{M}(X; Y)$  is convex and closed.

Note that condition (3) in Definition 5.2 is a restriction of condition (3') to the case  $\phi = 0$ .

In Appendix D we prove the following generalization of Corollary 5.2.

**Theorem 5.5:** For any robust monotone region  $\mathcal{M}$ , if the rate of statistically securely sampling  $(U, V)$  from  $(X, Y)$  is  $r > 0$ , then  $\mathcal{M}(X; Y) \subseteq r \cdot \mathcal{M}(U; V)$ .

Also, we can generalize Theorem 5.3 as follows.

**Theorem 5.6:**  $\mathfrak{T}$  is a (3-dimensional) robust monotone region (as in Definition 5.6).

**Proof:** We verify the four properties of a robust monotone region (see Definition 5.2 and Definition 5.6).

1) *Local computation cannot shrink it:* For all random variables with  $X - Y - Z$ , we need to show that  $\mathfrak{T}(X; YZ) \supseteq \mathfrak{T}(X; Y)$  and  $\mathfrak{T}(XY; Z) \supseteq \mathfrak{T}(X; Y)$ .

The first inclusion follows from the fact that for the joint p.m.f.  $p_{XYZQ} = p_{XYPZ|Y} p_{Q|XY}$ , we have

$$I(X; YZ|Q) = I(X; Y|Q)$$

$$I(Q; YZ|X) = I(Q; Y|X)$$

$$I(X; Q|YZ) = I(X; Q|Y).$$

2) *Communication cannot shrink it:* For all random variables  $(X, Y)$  and functions  $f$  over the support of



$X$  (resp.  $Y$ ), we have to show that  $\mathfrak{T}(X; (Y, f(X))) \supseteq \mathfrak{T}(X; Y)$  (resp.  $\mathfrak{T}((X, f(Y)); Y) \supseteq \mathfrak{T}(X; Y)$ ).

The first set inclusion follows from the following facts for the joint p.m.f.  $p_{XYZQ} = p_{XY}p_{Z|Y}p_{Q|XY}$ :

$$\begin{aligned} I(X; Y, f(X)|Q, f(X)) &= I(X; Y|Q, f(X)) \\ &\leq I(X; Y|Q) \\ I(X; Q, f(X)|Y, f(X)) &= I(X; Q|Y, f(X)) \\ &\leq I(X; Q|Y) \\ I(Y; Q, f(X)|X) &= I(Y; Q|X). \end{aligned}$$

3') *Statistically securely derived outputs do not have a much smaller region:* We let  $c = 1$ . Suppose  $I(X; V|U) \leq \phi$  and  $I(U; Y|V) \leq \phi$ . We shall show that  $\mathfrak{T}(U; V) \supseteq \mathfrak{T}(XU; VY) + \phi$ . For this, it is enough to show that, for any  $p_{Q|XUVY} \in \mathcal{P}_{XUVY}$ ,  $T(U; V|Q) \leq T(XU; VY|Q) + \phi$  (where the comparison is coordinate-wise and the addition applies to each coordinate). This is easy to see for the last coordinate since  $I(U; V|Q) \leq I(XU; VY|Q) \leq I(XU; VY|Q) + \phi$ . For the second coordinate, note that

$$\begin{aligned} I(XU; Q|VY) &\geq I(U; Q|VY) \\ &= I(U; QY|V) - I(U; Y|V) \\ &\geq I(U; Q|V) - I(U; Y|V). \end{aligned}$$

Since  $I(U; Y|V) \leq \phi$ , we have  $I(U; Q|V) \leq I(XU; Q|VY) + \phi$ . Similarly,  $I(V; Q|U) \leq I(VY; Q|XU) + \phi$ .

3'') Continuity follows from Theorem 2.5, with  $\hat{\delta}(\epsilon) = 2H_2(\epsilon) + \epsilon$  (so that  $\delta(\epsilon)$  in Theorem 2.5 is upper-bounded by  $\hat{\delta}(\epsilon) \log |\mathcal{X}||\mathcal{Y}|$ ). Convexity and closure follow from Theorem 2.3 and Theorem 2.4 respectively.

4) *Regions of independent pairs add up:* If  $(X_1, Y_1)$  is independent of  $(X_2, Y_2)$ , we have to show that  $\mathfrak{T}((X_1 X_2); (Y_1 Y_2)) = \mathfrak{T}(X_1; Y_1) + \mathfrak{T}(X_2; Y_2)$ . This follows easily from the following facts:

For the joint p.m.f.  $p_{X_1 Y_1 X_2 Y_2} p_{Q_1|X_1 Y_1} p_{Q_2|X_2 Y_2}$ , we have

$$\begin{aligned} I(X_1 X_2; Y_1 Y_2|Q_1 Q_2) &= I(X_1; Y_1|Q_1) + I(X_2 Y_2|Q_2) \\ I(X_1 X_2; Q_1 Q_2|Y_1 Y_2) &= I(X_1; Q_1|Y_1) + I(X_2; Q_2|Y_2) \\ I(Y_1 Y_2; Q_1 Q_2|X_1 X_2) &= I(Y_1; Q_1|X_1) + I(Y_2; Q_2|X_2) \end{aligned}$$

And, for the joint p.m.f.  $p_{X_1 Y_1 X_2 Y_2} p_{Q|X_1 Y_1 X_2 Y_2}$ , we have

$$\begin{aligned} I(X_1 X_2; Y_1 Y_2|Q) &\geq I(X_1; Y_1|Q) + I(X_2; Y_2|Q) \\ I(X_1 X_2; Q|Y_1 Y_2) &\geq I(X_1; Q|Y_1) + I(X_2; Q|Y_2) \\ I(Y_1 Y_2; Q|X_1 X_2) &\geq I(Y_1; Q|X_1) + I(Y_2; Q|X_2) \end{aligned}$$

Theorem 5.5 and Theorem 5.6 together yield a generalization of Corollary 5.4.

*Corollary 5.7:* If the rate of statistically securely sampling  $(U, V)$  from  $(X, Y)$  is  $r > 0$ , then  $\mathfrak{T}(X; Y) \subseteq r \cdot \mathfrak{T}(U; V)$ .

#### E. Bounding the Rate of Bit-OT from String-OT

Example 5.1 was contrived to highlight the shortcomings of prior work. We now give another example where the upperbound from our result strictly improves on prior work, but is further interesting for two reasons: firstly, the new example is based on natural correlated random variables that are widely studied (namely, variants of oblivious transfer), and secondly, the new upperbound we can prove actually matches an easy lowerbound and is therefore tight.

a) *Bit-Oblivious Transfer and String-Oblivious Transfer:* Oblivious Transfer, or OT [24], [25] is a pair of correlated random variables with great cryptographic significance. There are several variants of OT that have been considered in the literature. In particular, “bit-OT” corresponds to the following correlated pair of random variables:  $A = (S_1, S_2)$  and  $B = (C, S_C)$  where  $S_1, S_2$  are two i.i.d. uniformly random bits and the “choice bit”  $C$  is independent of  $(S_1, S_2)$  and takes a uniformly random values in  $\{1, 2\}$ . Informally, in bit-OT, one of the two bits that Alice gets is transferred to Bob, but Alice is oblivious to which one was chosen to be transferred.

It is well-known that qualitatively, the different forms of OT are all equivalent, in the sense that pairs of one variant can be securely sampled using pairs of another variant as set up (see for instance, [19]). However, the rate at which this can be done has not been studied well. That these rates are non-zero follows from a recent result in [16]. We are interested in upperbounding this rate (and indeed, when possible, calculating it exactly).

Consider the rate of sampling bit-OT from a generalization of bit-OT called “string-OT” where Alice receives two  $L$ -bit strings  $S_1, S_2$  instead of two bits (and one of those strings is obviously transmitted to Bob). It is not hard to see that the rate of sampling bit-OT from string-OT is 1, intuitively because a single instance of string-OT provides only one bit  $C$  that is hidden from Alice. (In terms of the monotones, the axis intercept  $T_1^{\text{int}}(A; B) = (1, 0, 0)$  for string-OT, independent of the length of the strings.) But what if we consider two string-OTs together, one in each direction? In this case, there are  $L$  bits with Bob that are hidden from Alice, and vice versa. We ask if we can sample OT from this set up at a rate larger than 1 (in particular, linear in  $L$ ).

Formally, we consider the set up  $(X, Y)$  and target random variables  $(U, V)$  as defined below.

Let  $S_{A,1}, S_{A,2}, S_{B,1}, S_{B,2} \in \{0, 1\}^L$  and  $C_A, C_B \in \{1, 2\}$  be six independent random variables all of which are uniformly distributed over their alphabets. Consider a pair of random variables  $X, Y$  defined as  $X = (C_A, S_{A,1}, S_{A,2}, S_{B,C_A})$  and  $Y = (C_B, S_{B,1}, S_{B,2}, S_{A,C_B})$ . (Note that  $(S_{A,1}, S_{A,2}, C_A)$  and  $(S_{B,1}, S_{B,2}, C_B)$  correspond to the two instances of  $L$ -bit string-OT, one in each direction.) Let  $U, V$  be a pair of random variables whose joint distribution is the same as that of  $X, Y$ , but with  $L = 1$ . In other words,  $U, V$  are a pair of independent bit-OT's in opposite directions.

It is easy to see that  $\mathfrak{T}(X; Y)$  intersects the coordinate axes at  $(1 + L, 0, 0)$ ,  $(0, 1 + L, 0)$ , and  $(0, 0, 2L)$ . From, these we can immediately obtain the upperbound of [29] on the efficiency, namely  $(1 + L)/2$ . Notice that this is dependent on  $L$  and would suggest that (several) long string-OT pairs can be turned into several (more) bit-OT pairs. However, as we show below, the efficiency of conversion is just 1, i.e., the best one can do is to turn each pair of string-OT's into a pair of bit-OT's.

To see this we need to consider a point on  $\mathfrak{T}(X; Y)$  other than the three axis intercepts. By setting  $Q = (C_A, C_B, S_{A,C_B}, S_{B,C_A})$  we get  $T(X; Y|Q) = (1, 1, 0)$ ; that is,  $\mathfrak{T}(X; Y)$  contains a point  $(1, 1, 0)$  independent of  $L$ . This already bounds the rate of sampling  $(U, V)$  from  $(X, Y)$  as set up, by some constant. To show that this constant is 1, we shall show that  $(1, 1, 0)$  occurs *on the boundary of*  $\mathfrak{T}(U; V)$ . Then it follows from Corollary 5.7 that the rate of (statistically) secure sampling is upperbounded by 1.

To show that  $(1, 1, 0)$  occurs on the boundary of  $\mathfrak{T}(U; V)$ , we show that  $\inf\{R_1 + R_2 : (R_1, R_2, 0) \in \mathfrak{T}(U; V)\} = 2$ . Since  $\mathfrak{T}(U; V)$  is a monotone region (Theorem 5.3), by property (4) of Definition 5.2, the regions of independent pairs add up. Hence, we need only characterize the  $\inf\{R_1 + R_2 : (R_1, R_2, 0) \in \mathfrak{T}(A; B)\}$ , where  $(A, B)$  is a single pair of independent bit-OT's:  $A = (S_1, S_2) \in \{0, 1\}^2$  uniformly distributed over its alphabet and  $B = (C, S_C)$ , where  $C \in \{1, 2\}$  is independent of  $A$  and uniformly distributed over its alphabet.

$$\begin{aligned} & \inf\{R_1 + R_2 : (R_1, R_2, 0) \in \mathfrak{T}(A; B)\} \\ &= \inf_{p_{Q|AB} \in \mathcal{P}_{X,Y}: I(A; B|Q)=0} I(B; Q|A) + I(A; Q|B) \\ &= H(A|B) + H(B|A) \\ &\quad - \sup_{p_{Q|AB} \in \mathcal{P}: I(A; B|Q)=0} H(A|QB) + H(B|QA). \end{aligned}$$

We show below that the sup term is 1. Since  $H(A|B) + H(B|A) = 2$ , this will allow us to conclude that the

smallest sum-rate  $R_1 + R_2$  such that  $(R_1, R_2, 0) \in \mathfrak{T}(A; B)$  is 1. Invoking the lemma above, the corresponding smallest sum-rate for  $U, V$  is then 2 as required.

To show that the sup term is 1, notice that the only valid choices of  $p_{Q|AB}$  are such that  $I(A; B|Q) = 0$ . This means that the resulting  $p_{AB|Q}(\cdot, \cdot|q)$  must belong to one of eight possible classes shown in Figure 7b (for any  $q$  with non-zero probability  $p_Q(q)$ ; we may assume that all  $q$ 's have non-zero probability without loss of generality). Recall that there is a cardinality bound on  $Q$ ; let us denote the alphabet of  $Q$  by  $\{q_1, q_2, \dots, q_N\}$ , where  $N$  is the cardinality bound.

We will first show that there is no loss of generality in assuming that no more than one of the  $q_i$ 's is such that its  $p_{AB|Q}(\cdot, \cdot|q_i)$  belongs to the same class (and hence we may take  $N = 8$ ). Suppose,  $q_1$  and  $q_2$  belong to the same class, say class 1, with parameters  $p_1$  and  $p_2$  respectively. Then, if we denote the binary entropy function by  $H_2(\cdot)$ , we have

$$\begin{aligned} & H(A|QB) + H(B|QA) \\ &= \sum_{k=1}^N p_Q(q_k) (H(A|BQ = q_k) + H(B|AQ = q_k)) \\ &= p_Q(q_1)H_2(p_1) + p_Q(q_2)H_2(p_2) \\ &\quad + \sum_{k=3}^N p_Q(q_k) (H(A|BQ = q_k) + H(B|AQ = q_k)) \\ &\leq (p_Q(q_1) + p_Q(q_2)) H_2\left(\frac{p_Q(q_1)p_1 + p_Q(q_2)p_2}{p_Q(q_1) + p_Q(q_2)}\right) \\ &\quad + \sum_{k=3}^N p_Q(q_k) (H(A|BQ = q_k) + H(B|AQ = q_k)), \end{aligned}$$

where the inequality (Jensen's) follows from the concavity of the binary entropy function. Thus, we can define a  $Q'$  of alphabet size  $N - 1$  where letters  $q_1, q_2$  are replaced by  $q_0$  such that  $p_{Q'}(q_0) = p_Q(q_1) + p_Q(q_2)$ , and  $p_{AB|Q'=q_0}$  is in class 1 with parameter  $\frac{p_Q(q_1)p_1 + p_Q(q_2)p_2}{p_Q(q_1) + p_Q(q_2)}$ , while maintaining for  $i = 3, \dots, N$ ,  $p_{Q'}(q_i) = p_Q(q_i)$  and  $p_{AB|Q'}(a, b|q_i) = p_{AB|Q}(a, b|q_i)$ . (It is easy to verify (a) that this gives a valid joint p.m.f. for  $p_{ABQ'}$ , (b) that the induced  $p_{AB}$  is the same as the original, and (c) that the induced  $p_{Q'|AB}$  satisfies the condition  $I(A; B|Q') = 0$ .) Then, the above inequality states that

$$H(A|QB) + H(B|QA) \leq H(AQ'B) + H(B|Q'A)$$

proving our claim.

Thus, without loss of generality, we may assume that

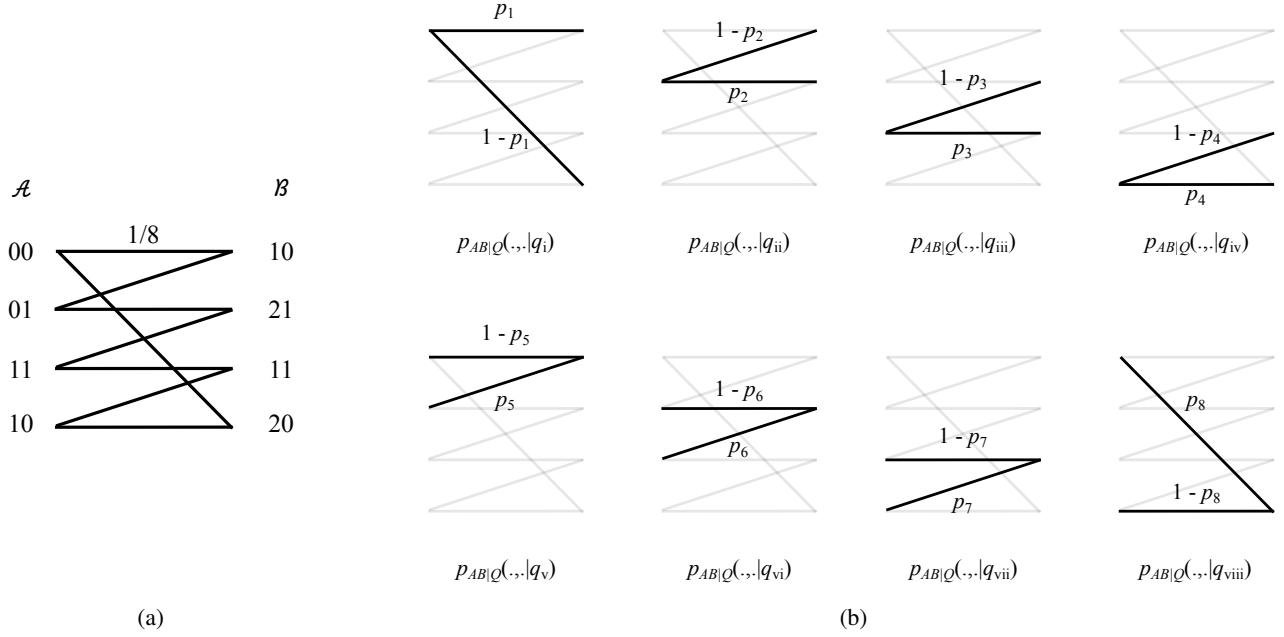


Fig. 7: (a) Joint p.m.f. of  $A, B$ . Each solid line represents a probability mass of  $1/8$ . (b) Eight possible classes that  $p_{AB|Q}(\cdot, \cdot | q)$  may belong to for a  $p_{Q|AB}$  which satisfies  $I(A; B|Q) = 0$ .

$N = 8$  and  $p_{AB|Q}(\cdot, \cdot | q_i)$  belongs to class  $i$ . Notice that

$$\begin{aligned}
 p_{Q|AB}(q_1|00, 10) + p_{Q|AB}(q_5|00, 10) &= 1, \\
 p_{Q|AB}(q_2|01, 10) + p_{Q|AB}(q_5|01, 10) &= 1, \\
 p_{Q|AB}(q_2|01, 21) + p_{Q|AB}(q_6|01, 21) &= 1, \\
 p_{Q|AB}(q_3|11, 21) + p_{Q|AB}(q_6|11, 21) &= 1, \\
 p_{Q|AB}(q_3, 11, 11) + p_{Q|AB}(q_7|11, 11) &= 1, \\
 p_{Q|AB}(q_4|10, 11) + p_{Q|AB}(q_7|10, 11) &= 1, \\
 p_{Q|AB}(q_4|10, 20) + p_{Q|AB}(q_8|10, 20) &= 1, \\
 p_{Q|AB}(q_1|00, 20) + p_{Q|AB}(q_8|00, 20) &= 1.
 \end{aligned}$$

Let us define

$$\begin{aligned}
 \tilde{p}_1 &\triangleq p_{Q|AB}(q_1|00, 10), & \tilde{p}_5 &\triangleq p_{Q|AB}(q_5|01, 10), \\
 \tilde{p}_2 &\triangleq p_{Q|AB}(q_2|01, 21), & \tilde{p}_6 &\triangleq p_{Q|AB}(q_6|11, 21), \\
 \tilde{p}_3 &\triangleq p_{Q|AB}(q_3|11, 11), & \tilde{p}_7 &\triangleq p_{Q|AB}(q_7|10, 11), \\
 \tilde{p}_4 &\triangleq p_{Q|AB}(q_4|10, 20), & \tilde{p}_8 &\triangleq p_{Q|AB}(q_8|00, 20).
 \end{aligned}$$

Let us evaluate  $H(B|QA)$  in terms of the above parameters. Notice that  $H(B|Q = q_i, A) = 0$  for  $i = 5, \dots, 8$ . Hence

$$\begin{aligned}
 H(B|QA) &= \sum_{(q,a) \in \{(1,00), (2,01), (3,11), (4,10)\}} p_{QA}(q, a) H(B|Q = q, A = a) \\
 &= \frac{\tilde{p}_1 + (1 - \tilde{p}_8)}{8} H_2\left(\frac{\tilde{p}_1}{\tilde{p}_1 + (1 - \tilde{p}_8)}\right)
 \end{aligned}$$

$$\begin{aligned}
 &+ \frac{\tilde{p}_2 + (1 - \tilde{p}_5)}{8} H_2\left(\frac{\tilde{p}_2}{\tilde{p}_2 + (1 - \tilde{p}_5)}\right) \\
 &+ \frac{\tilde{p}_3 + (1 - \tilde{p}_6)}{8} H_2\left(\frac{\tilde{p}_3}{\tilde{p}_3 + (1 - \tilde{p}_6)}\right) \\
 &+ \frac{\tilde{p}_4 + (1 - \tilde{p}_7)}{8} H_2\left(\frac{\tilde{p}_4}{\tilde{p}_4 + (1 - \tilde{p}_7)}\right) \\
 &\leq \frac{4 + \sum_{i=1}^4 \tilde{p}_i - \sum_{j=5}^8 \tilde{p}_j}{8},
 \end{aligned}$$

where the inequality follows from the fact that binary entropy function is upperbounded by 1. Similarly, we can get

$$H(A|QB) \leq \frac{4 + \sum_{j=5}^8 \tilde{p}_j - \sum_{i=1}^4 \tilde{p}_i}{8}.$$

Combining, we obtain, as desired,

$$H(B|QA) + H(A|QB) \leq 1.$$

*Remark:* Note that we have actually shown that for bit-OT  $(A, B)$ , the intersection of  $\mathfrak{T}(A; B)$  on the plane  $z = 0$  is the increasing hull of the line segment between  $(1, 0, 0)$  and  $(0, 1, 0)$ . This follows from what we showed above (i.e.,  $\inf\{R_1 + R_2 : (R_1, R_2, 0) \in \mathfrak{T}(A; B)\} = 1$ ) combined with the fact that  $T_1^{\text{int}}(A; B) = (1, 0, 0)$  and  $T_2^{\text{int}}(A; B) = (0, 1, 0)$ , and that  $\mathfrak{T}(A; B)$  is convex.

#### ACKNOWLEDGEMENTS

The first author would like to gratefully acknowledge discussions with Venkat Anantharam, Péter Gács, and

Young-Han Kim. We also thank Hemanta Maji and Mike Rosulek for discussions at an early stage in this work. The example in Section V-E is based on a suggestion by Jürg Wullschleger. This work was supported in part by a Ramanujan Fellowship of the Department of Science and Technology, Government of India, and NSF CAREER award 07-47027.

## REFERENCES

- [1] R. Ahlswede and J. Körner, “On common information and related characteristics of correlated information sources,” in *Proc. of the 7th Prague Conference on Information Theory*, 1974.
- [2] D. Beaver, “Correlated pseudorandomness and the complexity of private computations,” in *Proc. 28th STOC*, pp. 479–488. ACM, 1996.
- [3] D. Beaver, “Precomputing oblivious transfer,” in Don Coppersmith, editor, *CRYPTO*, vol. 963 of *Lecture Notes in Computer Science*, pp. 97–109. Springer, 1995.
- [4] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2ed, Wiley, 2006.
- [5] I. Csiszár and R. Ahlswede, “On oblivious transfer capacity,” in *Proc. International Symposium on Information Theory (ISIT)*, pp. 2061–2064, 2007.
- [6] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Akadémiai Kiadó, Budapest, 1981.
- [7] Y. Dodis and S. Micali, “Lower bounds for oblivious transfer reductions,” in Jacques Stern, editor, *EUROCRYPT*, vol. 1592 of *Lecture Notes in Computer Science*, pp. 42–55. Springer, 1999.
- [8] A. El Gamal and Y.-H. Kim, *Network Information Theory*, Cambridge, 2012.
- [9] P. Gács and J. Körner, “Common information is far less than mutual information,” *Problems of Control and Information Theory*, 2(2):119–162, 1973.
- [10] M. Gastpar, B. Rimoldi, and M. Vetterli, “To code or not to code: Lossy source-channel communication revisited,” *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1147–1158, 2003.
- [11] R. M. Gray and A. D. Wyner, “Source coding for a simple network,” *Bell System Technical Journal*, vol. 53, pp. 1681–1721, 1974.
- [12] H. Imai, K. Morozov, and A. C. A. Nascimento, “On the oblivious transfer capacity of the erasure channel,” in *Proc. International Symposium on Information Theory (ISIT)*, pp. 1428–1431, 2006.
- [13] H. Imai, K. Morozov, and A. C. A. Nascimento, “Efficient oblivious transfer protocols achieving a non-zero rate from any non-trivial noisy correlation,” in *Proc. International Conference on Information Theoretic Security (ICITS)*, 2007.
- [14] H. Imai, K. Morozov, A. C. A. Nascimento, and A. Winter, “Efficient protocols achieving the commitment capacity of noisy correlations,” in *Proc. International Symposium on Information Theory (ISIT)*, pp. 1432–1436, 2006.
- [15] H. Imai, J. Müller-Quade, A. C. A. Nascimento, and A. Winter, “Rates for bit commitment and coin tossing from noisy correlation,” in *Proc. International Symposium on Information Theory (ISIT)*, pp. 45–, 2004.
- [16] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, “Extracting Correlations,” in *Proc. FOCS*, pp. 261–270. IEEE, 2009.
- [17] S. Kamath and V. Anantharam, “A new dual to the Gács-Körner common information defined via the Gray-Wyner system,” in *Proc. 48th Allerton Conf. on Communication, Control, and Computing*, pp. 1340–1346, 2010.
- [18] J. Kilian, “Founding cryptography on oblivious transfer,” in *Proc. STOC*, pp. 20–31. ACM, 1988.
- [19] J. Kilian, “More general completeness theorems for secure two-party computation,” in *Proc. 32nd STOC*, pp. 316–324. ACM, 2000.
- [20] D. Marco and M. Effros, “On lossless coding with coded side information,” *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3284–3296, 2009.
- [21] L. Nachbin, *Topology and Order*, D. Van Nostrand, 1965.
- [22] V. M. Prabhakaran and M. M. Prabhakaran, “Assisted common information,” in *Proc. International Symposium on Information Theory (ISIT)*, pp. 2602–2606, 2010. Extended draft available at <http://arxiv.org/abs/1002.1916>.
- [23] V. M. Prabhakaran and M. M. Prabhakaran, “Assisted common information: Further results,” in *Proc. International Symposium on Information Theory (ISIT)*, pp. 2861 – 2865, 2011. Extended draft available at <http://arxiv.org/pdf/1105.6163>.
- [24] M. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.
- [25] Stephen Wiesner. “Conjugate coding,” *Sigact News*, vol. 15, pp. 78–88, 1983.
- [26] S. Winkler and J. Wullschleger. “Statistical impossibility results for oblivious transfer reductions,” *Cryptology ePrint Archive*, Report 2009/508, 2009. <http://eprint.iacr.org/>.
- [27] A. Winter, A. C. A. Nascimento, and H. Imai. “Commitment capacity of discrete memoryless channels,” In Kenneth G. Paterson, editor, *IMA Int. Conf.*, vol. 2898 of *Lecture Notes in Computer Science*, pp. 35–51. Springer, 2003.
- [28] H. S. Witsenhausen, “On sequences of pairs of dependent random variables,” *SIAM Journal of Applied Mathematics*, 28:100–113, 1975.
- [29] S. Wolf and J. Wullschleger. “New monotones and lower bounds in unconditional two-party computation,” *IEEE Transactions on Information Theory*, 54(6):2792–2797, 2008.
- [30] J. Wullschleger. Oblivious-Transfer Amplification. Ph.D. thesis, Swiss Federal Institute of Technology, Zürich. <http://arxiv.org/abs/cs.CR/0608076>.
- [31] A. D. Wyner, “The common information of two dependent random variables,” *IEEE Transactions on Information Theory*, 21(2):163–179, 1975.
- [32] A. D. Wyner and J. Ziv, “Rate-distortion function for source coding with side information at the decoder,” *IEEE Transactions on Information Theory*, 22(1):1–11, 1976.
- [33] H. Yamamoto, “Coding theorems for Shannon’s cipher system with correlated source outputs, and common information,” *IEEE Transactions on Information Theory*, 40(1):85–95, 1994.

## APPENDIX A

### DETAILS OMITTED FROM SECTION II

**Lemma A.1:** Given a pair of random variables  $(X, Y)$  and a p.m.f.  $p_{Q|XY}$  such that  $I(Y; Q|X) = I(X; Q|Y) = 0$ , there exists a p.m.f.  $p_{Q'|XY}$  such that  $H(Q'|X) = H(Q'|Y) = 0$  and  $Q - Q' - XY$ .

**Proof:** Suppose  $p_{Q|XY}$  is such that  $I(Y; Q|X) = I(X; Q|Y) = 0$ . Then

$$p_{Q|XY}(q|x, y) = p_{Q|X}(q|x) = p_{Q|Y}(q|y).$$

Hence, for all  $(x, y)$  such that  $p_{XY}(x, y) > 0$ , we must have  $\forall q$ ,  $p_{Q|X}(q|x) = p_{Q|Y}(q|y)$ . This implies that, in

The following simple information theoretic identities for three jointly distributed random variables  $X, Y, Q$  are used at several places in this paper.

$$I(Y; Q|X) = I(XY; Q) - I(X; Q) = H(X|Q) + I(XY; Q) - H(X), \quad (49)$$

$$I(X; Q|Y) = I(XY; Q) - I(Y; Q) = H(Y|Q) + I(XY; Q) - H(Y), \quad (50)$$

$$I(X; Y|Q) = H(X|Q) + H(Y|Q) - H(XY|Q) = H(X|Q) + H(Y|Q) + I(XY; Q) - H(XY), \quad (51)$$

$$I(X; Y|Q) = I(X; Y) + I(Y; Q|X) + I(X; Q|Y) - I(XY; Q).. \quad (52)$$

The first three equalities are easy to follow. The last one can be obtained by subtracting the first two from the third.

the characteristic bipartite graph (which has vertices in  $\mathcal{X} \cup \mathcal{Y}$  and an edge between  $x \in \mathcal{X}$  and  $y \in \mathcal{Y}$  if and only if  $p_{XY}(x, y) > 0$ ), for each connected component  $C \subseteq \mathcal{X} \cup \mathcal{Y}$ , there is a distribution  $p_Q^C$  such that for all  $x \in C \cap \mathcal{X}$  and all  $q$ ,  $p_{Q|X}(q|x) = p_Q^C(q)$ ; similarly, for all  $y \in C \cap \mathcal{Y}$  and all  $q$ ,  $p_{Q|Y}(q|y) = p_Q^C(q)$ . Define  $p_{Q'|XY}$  over the set of connected components in this graph such that, with probability 1  $Q'$  is the connected component  $C(X, Y)$  in this graph to which the vertices  $X$  and  $Y$  belong (and hence  $H(Q'|X) = H(Q'|Y) = 0$ ), and  $p_{Q|Q'}(q|C) = p_Q^C(q)$ . Then  $p_{Q|XY}(q|x, y) = p_{Q|X}(q|x) = p_Q^{C(x,y)}(q) = p_{Q|Q'}(q|C(x, y))$ , so that  $Q - Q' - XY$ . ■

The following calculation is useful in applying the above lemma in a couple of our proofs.

**Lemma A.2:** For correlated random variables  $(X, Y, Q, Q')$  if  $H(Q'|X) = H(Q'|Y) = 0$  and  $Q - Q' - XY$ , then  $I(X; Y|Q') \leq I(X; Y|Q)$ .

*Proof:* Note that (52) gives

$$I(X; Y|Q) = I(X; Y) - I(XY; Q) + I(Y; Q|X) + I(X; Q|Y).$$

Since,  $H(Q'|X) = H(Q'|Y) = 0$ , we have

$$I(X; Y|Q') = I(X; Y) - I(XY; Q').$$

Also,  $I(XY; Q) \leq I(XY; QQ') = I(XY; Q')$  where we used the fact that  $Q - Q' - XY$  and hence  $I(XY; QQ') = I(XY; Q') + I(XY; Q|Q') = I(XY; Q')$ . Thus  $I(X; Y|Q) - I(X; Y|Q') = I(Y; Q|X) + I(X; Q|Y) - I(XY; Q) + I(XY; Q') \geq 0$ . ■

**Proof of Theorem 2.2:** To prove (5), firstly note that  $T_1^{\text{int}}(X; Y) =$

$$\inf_{\substack{p_{Q|XY}: \\ I(X; Q|Y)=0 \\ I(X; Y|Q)=0}} I(Y; Q|X) \leq \inf_{\substack{p_{Q|XY}: \\ H(Q|X)=0 \\ I(X; Y|Q)=0}} H(Q|X),$$

because if  $H(Q|Y) = 0$  then  $I(X; Q|Y) = 0$  and  $I(Y; Q|X) = H(Q|X)$ . For the other direction, we

invoke Lemma A.1 (with  $X$  and  $Q$  interchanged), so that given  $Q$  such that  $I(X; Q|Y) = I(X; Y|Q) = 0$ ,  $\exists Q'$  such that  $H(Q'|Y) = H(Q'|Q) = 0$  and  $X - Q' - QY$ ; then  $H(Q'|X) = I(Y; Q'|X) \leq I(Y; Q|X)$ , and  $X - Q' - Y$ . So  $Q'$  is considered in the inf expression of the RHS, and we have LHS  $\geq$  RHS. This proves (5). Similarly, (6) holds.

To prove (7), firstly we note that  $T_3^{\text{int}}(X; Y) =$

$$\inf_{\substack{p_{Q|XY}: \\ I(Y; Q|X)=0 \\ I(X; Q|Y)=0}} I(X; Y|Q) \leq \inf_{\substack{p_{Q|XY}: \\ H(Q|X)=0 \\ H(Q|Y)=0}} I(X; Y|Q),$$

since  $H(Q|X) = H(Q|Y) = 0$  implies that  $I(Y; Q|X) = I(X; Q|Y) = 0$ . For the inequality in the other direction, by Lemma A.1, given  $Q$  such that  $I(Y; Q|X) = I(X; Q|Y) = 0$ , we get  $Q'$  such that  $H(Q'|X) = H(Q'|Y) = 0$  and  $Q - Q' - XY$ ; then, by Lemma A.2 it follows that  $I(X; Y|Q) \geq I(X; Y|Q')$ . Hence,  $\inf_{p_{Q|XY}: I(Y; Q|X)=I(X; Q|Y)=0} I(X; Y|Q) \geq \inf_{p_{Q|XY}: H(Q|X)=H(Q|Y)=0} I(X; Y|Q)$ . Thus, (7) holds. ■

**Proof of Theorem 2.3:** Consider any two points  $s_1, s_2 \in \mathfrak{T}(X; Y)$ . Consider any point  $s = \alpha s_1 + (1 - \alpha)s_2$  for  $0 \leq \alpha \leq 1$ . We need to show that  $s \in \mathfrak{T}(X; Y)$  as well.

Since  $s_1, s_2 \in \mathfrak{T}(X; Y)$ , there are random variables  $p_{Q_1|XY}$  and  $p_{Q_2|XY}$  such that  $s'_1 := T(X; Y|Q_1) \leq s_1$  and  $s'_2 := T(X; Y|Q_2) \leq s_2$ . Let  $J$  be a binary random variable independent of  $(X, Y, Q_1, Q_2)$  taking on value 1 with probability  $\alpha$  and 2 with probability  $1 - \alpha$ . Let  $Q = (J, Q_J)$ . Then  $T(X; Y|Q) = \alpha T(X; Y|Q_1) + (1 - \alpha)T(X; Y|Q_2)$ . That is,  $s' = \alpha s'_1 + (1 - \alpha)s'_2$  is in  $\mathfrak{T}(X; Y)$ . Hence  $s \in \mathfrak{T}(X; Y)$ , since  $s \geq s'$ . ■

**Lemma A.3:** If  $A \subseteq \mathbb{R}^m$  is compact, then its increasing hull,

$$i(A) = \{x \in \mathbb{R}^m : x \geq a \text{ for some } a \in A\},$$

is closed.

**Proof:** Our proof of this simple fact is along the lines of [21, Proposition 4, pg. 44]. Consider an arbitrary

point  $a \in \mathbb{R}^m - i(A)$ . We will show that there exists a neighbourhood  $V$  of  $a$  such that  $V \cap i(A) = \emptyset$ .

For any point  $x \in A$ , we have  $a \not\geq x$  (coordinate-wise); i.e., for some  $j \in \{1, \dots, m\}$ ,  $a_j < x_j$ . Let  $\ell = x_j - a_j$ . Let  $V_x = \{a' : \|a' - a\| < \ell/3\}$  and  $W_x = \{x' : \|x' - x\| < \ell/3\}$  be neighbourhoods around  $a$  and  $x$ . Then  $V_x \cap i(W_x) = \emptyset$  (for any  $a' \in V_x$  and  $x'' \in i(W_x)$ , we have  $a' \neq x''$ , because,  $a'_j < a_j + \ell/3 < x_j - \ell/3$ , but since  $x'' \geq x'$  for some  $x' \in W_x$ ,  $x''_j \geq x'_j > x_j - \ell/3$ ).

Since  $\{W_x : x \in A\}$  is an open cover of  $A$ ,  $A$  being compact implies that there is a finite  $n$  and  $x_1, \dots, x_n$  such that

$$A \subseteq \bigcup_{k=1}^n W_{x_k},$$

which in turn implies that

$$i(A) \subseteq \bigcup_{k=1}^n i(W_{x_k}).$$

Let

$$V = \bigcap_{k=1}^n V_{x_k}.$$

Clearly,  $V$  is a neighbourhood of  $a$  and we have

$$V \cap i(A) = \bigcup_{k=1}^n V \cap i(W_{x_k}) = \emptyset.$$

Hence  $i(A)$  is closed.  $\blacksquare$

The following simple (and standard) observation is used in proving Lemma 2.6.

*Lemma A.4:* If  $p_Z$  and  $p_{Z'}$  are such that  $\Delta(Z, Z') = \epsilon$ , then there is a joint distribution  $p_{JWW'}$  such that  $p_W = p_Z$ ,  $p_{W'} = p_{Z'}$ ,  $p_J(0) = \epsilon$  and  $p_J(1) = 1 - \epsilon$  and  $J = 1 \implies W = W'$ .

*Proof:* First we define independent random variables  $J$ ,  $W_0$ ,  $W_1$  and  $W_2$  (the first one over  $\{0, 1\}$  and the others over the common alphabet of  $Z$  and  $Z'$  as follows.

$$\begin{aligned} p_J(0) &= \epsilon, \text{ and } p_J(1) = 1 - \epsilon, \\ p_{W_0}(z) &= \frac{\min\{p_Z(z), p_{Z'}(z)\}}{1 - \epsilon}, \\ p_{W_1}(z) &= \frac{p_Z(z) - (1 - \epsilon) \cdot p_{W_0}(z)}{\epsilon}, \\ p_{W_2}(z) &= \frac{p_{Z'}(z) - (1 - \epsilon) \cdot p_{W_0}(z)}{\epsilon}. \end{aligned}$$

We define  $W$  and  $W'$  in terms of these random variables: when  $J = 1$ ,  $W = W' = W_0$ , and when  $J = 0$  we set  $W = W_1$  and  $W' = W_2$ . It is easy to verify that the resulting random variables have the correct marginals.  $\blacksquare$

*Lemma 2.6:* Suppose random variables  $(A, B, C)$  and  $(A', B', C')$  over the same alphabet  $\mathcal{A} \times \mathcal{B} \times \mathcal{C}$  are such that  $\Delta(ABC, A'B'C') = \epsilon$ . Then  $I(A'; B'|C') \leq I(A; B|C) + 2H_2(\epsilon) + \epsilon \log \min\{|\mathcal{A}|, |\mathcal{B}|\}$ .

*Proof:* We apply Lemma A.4 with  $Z = (A, B, C)$  and  $Z' = (A', B', C')$  to obtain a joint distribution  $p_{J,A,B,C,A',B',C'}$  so that  $J = 1 \implies (A, B, C) = (A', B', C')$  and this event occurs with probability  $1 - \epsilon$ .

Now, note that

$$\begin{aligned} I(A; B|C) &= I(A; BJ|C) - I(A; J|BC) \\ &= I(A; B|CJ) + I(A; J|C) - I(A; J|BC). \end{aligned}$$

Since  $0 \leq I(A; J|C) \leq H(J)$  and  $0 \leq I(A; J|BC) \leq H(J)$ , we have

$$|I(A; B|C) - I(A; B|CJ)| \leq H(J) = H_2(\epsilon) \quad (53)$$

The same condition holds for  $A', B', C'$  instead of  $A, B, C$ . Hence

$$\begin{aligned} I(A'; B'|C') &\leq I(A'; B'|C'J) + H_2(\epsilon) \\ &= (1 - \epsilon)I(A'; B'|C', J = 1) \\ &\quad + \epsilon I(A'; B'|C', J = 0) + H_2(\epsilon) \\ &= (1 - \epsilon)I(A; B|C, J = 1) \\ &\quad + \epsilon I(A'; B'|C', J = 0) + H_2(\epsilon) \\ &= I(A; B|CJ) - \epsilon I(A; B|C, J = 0) \\ &\quad + \epsilon I(A'; B'|C', J = 0) + H_2(\epsilon) \\ &\stackrel{(a)}{\leq} I(A; B|C) + \epsilon I(A'; B'|C', J = 0) + 2H_2(\epsilon) \\ &\leq I(A; B|C) + \epsilon \min\{\log |\mathcal{A}|, \log |\mathcal{B}|\} + 2H_2(\epsilon), \end{aligned}$$

where (a) follows from (53).  $\blacksquare$

## APPENDIX B DETAILS OMITTED FROM SECTION III

*Proof of Corollary 3.2:* The first equation (12) follows immediately from Theorem 3.1. We need to show (13) which is repeated below for convenience.

$$\mathfrak{T}(X; Y) = i(f_{X,Y}(\mathcal{R}_{\text{ACI}}(X; Y))) \quad (13)$$

where  $f_{X,Y}$  is an affine map defined as

$$f_{X,Y} \left( \begin{bmatrix} R_1 \\ R_2 \\ R_{\text{CI}} \end{bmatrix} \right) \triangleq \begin{bmatrix} R_1 \\ R_2 \\ I(X; Y) + R_1 + R_2 - R_{\text{CI}} \end{bmatrix}.$$

Given a  $p_{Q|XY}$  and  $(r_1, r_2, r_{\text{CI}})$  such that  $r_1 \geq I(Y; Q|X)$ ,  $r_2 \geq I(X; Q|Y)$  and  $r_{\text{CI}} \leq I(XY; Q)$ , we have

$$\begin{aligned} &r_1 + r_2 - r_{\text{CI}} + I(X; Y) \\ &\geq I(Y; Q|X) + I(X; Q|Y) - I(XY; Q) + I(X; Y) \\ &= I(X; Y|Q), \end{aligned}$$

where the last equality is (52). Thus, L.H.S.  $\supseteq$  R.H.S.

If  $(r'_1, r'_2, r'_3) \in \mathfrak{T}(X; Y)$ , then there is a  $p_{Q|XY}$  such that  $r'_1 \geq I(Y; Q|X)$ ,  $r'_2 \geq I(X; Q|Y)$  and  $r'_3 \geq I(X; Y|Q)$ . But, since (52) implies that  $(I(Y; Q|X), I(X; Q|Y), I(X; Y|Q)) \in f_{X,Y}(\mathcal{R}_{\text{ACI}}(X; Y))$ , we have  $(r'_1, r'_2, r'_3) \in i(f_{X,Y}(\mathcal{R}_{\text{ACI}}(X; Y)))$ . Thus, L.H.S.  $\subseteq$  R.H.S.  $\blacksquare$

*Proof of Corollary 3.3:*

From the definitions it is clear that,  $C_{\text{GK}}(X; Y) \leq \mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y)$ . But as we will show, this is in fact an equality. Theorem 3.1 implies that

$$\mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y) = \max_{\substack{p_{Q|XY}: \\ I(X; Q|Y)=I(Y; Q|X)=0}} I(XY; Q). \quad (54)$$

By Lemma A.1, given  $p_{Q|XY}$  such that  $I(X; Q|Y) = I(Y; Q|X) = 0$ , we can find a random variable  $Q'$  with  $H(Q'|X) = H(Q'|Y) = 0$  and  $Q - Q' - (X, Y)$  is a Markov chain. Then, clearly,  $I(X; Q'|Y) = I(Y; Q'|X) = 0$  and furthermore

$$I(XY; Q) \leq I(XY; QQ') = I(XY; Q') = H(Q').$$

Hence,

$$\mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y) = \max_{p_{Q'|XY}: H(Q'|X)=H(Q'|Y)=0} H(Q').$$

Since  $H(Q'|X) = H(Q'|Y) = 0$ ,  $Q' = f_1(X)$  and  $Q' = f_2(Y)$  for some functions  $f_1$  and  $f_2$ , and hence  $C_{\text{GK}}(X; Y) \geq H(Q')$ . So,  $C_{\text{GK}}(X; Y) \geq \mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y)$ . Hence, we can conclude (14)-(15).

It only remains to show

$$T_3^{\text{int}}(X; Y) = I(X; Y) - \mathcal{R}_{\text{ACI},3}^{\text{int}}(X; Y). \quad (55)$$

This easily follows from (4) and (54) using (49)-(51).  $\blacksquare$

*Proof of Lemma 3.5:*

We are given  $p_{X,Y}$ ,  $p_{Q|XY}^*$ ,  $d$ . Also, we have

$$D^* = \mathbb{E}_{p_{X,Y} p_{Q|XY}^*} [d(X, Y, Q)].$$

This proof uses the notion of typicality. We will use notation, definitions, and results from [8]. All typical sequences are defined with respect to the joint distribution  $p_{X,Y} p_{Q|XY}^*$ . For a positive integer  $k$ , we will denote  $\{1, \dots, k\}$  by  $[k]$ .

*Random codebook construction:* Let  $\epsilon' > 0$  and  $p_Q(q) = \sum_{x,y} p_{X,Y}(x, y) p_{Q|XY}^*(q|x, y)$  be the marginal distribution of  $Q$  induced by the given joint distribution. Let  $r, r_1, r_2$  be such that  $r \geq r_1, r_2$ . We generate  $2^{nr}$  codewords  $Q^n(l), l \in [2^{nr}]$  randomly and independently each according to  $\prod_{i=1}^n p_Q(q_i)$ . The set of indices  $l \in [2^{nr}]$  is then partitioned in two different ways into equal

size subsets: *1-bins*  $\mathcal{B}_1(m_1) = \{(m_1 - 1)2^{n(r-r_1)} + 1, \dots, m_1 2^{n(r-r_1)}\}, m_1 \in [2^{nr_1}]$ , and *2-bins*  $\mathcal{B}_2(m_2) = \{(m_2 - 1)2^{n(r-r_2)} + 1, \dots, m_2 2^{n(r-r_2)}\}, m_2 \in [2^{nr_2}]$ .

*Encoding:* If the input to the encoder is  $(x^n, y^n)$ , it finds an index  $l$  such that  $(x^n, y^n, q^n(l)) \in \mathcal{T}_{\epsilon'}^{(n)}(X, Y, Q)$ . If none is available,  $l$  is chosen uniformly at random from  $[2^{nr}]$ . The encoder sends to the  $k$ -th receiver,  $k = 1, 2$ , the bin index  $m_k$  such that  $l \in \mathcal{B}_k(m_k)$ , i.e.,  $f_k^{(n)}(x^n, y^n) = m_k, k = 1, 2$ .

*Decoding:* The first decoder, on receiving  $m_1$ , tries to find a unique  $\hat{l}_1 \in \mathcal{B}_1(m_1)$  such that  $(x^n, q^n(\hat{l}_1)) \in \mathcal{T}_{\epsilon'}^{(n)}(X, Q)$ . If it cannot find such an  $\hat{l}_1$ , it sets  $\hat{l}_1 = 1$ . Decoder 1 outputs  $\hat{l}_1$ , i.e.,  $g_1^{(n)}(x^n, m_1) = \hat{l}_1$ . Similarly, decoder 2 outputs a  $\hat{l}_2$  it finds using  $y^n, m_2$ , and  $\mathcal{B}_2$ .

*Reconstruction:* The reconstruction function  $h^{(n)}$  is defined as  $h^{(n)}(l) = q^n(l)$ . Thus the output sequence is

$$q^n = h^{(n)}(\hat{l}_1) = q^n(\hat{l}_1).$$

*Analysis of the probability of error and expected distortion:* Let  $L, M_1, M_2, \hat{L}_1, \hat{L}_2$  be the indices chosen by the encoder and the decoder. We define the *error event* as

$$\mathcal{E} =$$

$$\{\hat{L}_1 \neq \hat{L}_2\} \cup \{(X^n, Y^n, Q^n(\hat{L}_1)) \notin \mathcal{T}_{\epsilon'}^{(n)}(X, Y, Q)\}.$$

Let

$$\mathcal{E}_0 = \{(X^n, Y^n, Q^n(l)) \notin \mathcal{T}_{\epsilon'}^{(n)} \text{ for all } l \in [2^{nr}]\},$$

$$\mathcal{E}_1 = \{(X^n, Q^n(\tilde{l}_1)) \in \mathcal{T}_{\epsilon'}^{(n)} \text{ for some}$$

$$\tilde{l}_1 \in \mathcal{B}_1(M_1), \tilde{l}_1 \neq L\},$$

$$\mathcal{E}_2 = \{(Y^n, Q^n(\tilde{l}_2)) \in \mathcal{T}_{\epsilon'}^{(n)} \text{ for some}$$

$$\tilde{l}_2 \in \mathcal{B}_2(M_2), \tilde{l}_2 \neq L\}.$$

Since the error event occurs only when  $(X^n, Y^n, Q^n(L)) \notin \mathcal{T}_{\epsilon'}^{(n)}$  or at least one of  $L_1$  and  $L_2$  is different from  $L$ , we have

$$\mathcal{E} \subseteq \mathcal{E}_0 \cup \mathcal{E}_1 \cup \mathcal{E}_2.$$

By union bound,

$$\Pr(\mathcal{E}) \leq \Pr(\mathcal{E}_0) + \Pr(\mathcal{E}_1) + \Pr(\mathcal{E}_2).$$

By covering lemma [8, Lemma 3.3],  $\Pr(\mathcal{E}_0) \rightarrow 0$  as  $n \rightarrow \infty$  provided  $r > I(X, Y; Q) + \delta(\epsilon')$ , where  $\delta(\epsilon') \downarrow 0$  as  $\epsilon' \downarrow 0$ . To upperbound  $\Pr(\mathcal{E}_1)$ , we claim that

$$\Pr(\mathcal{E}_1) \leq \Pr\left(\{(X^n, Q^n(\tilde{l}_1)) \in \mathcal{T}_{\epsilon'}^{(n)} \text{ for some } \tilde{l}_1 \in \mathcal{B}_1(1)\}\right).$$

For a proof see [8, Lemma 11.1, pg. 284]. For each  $\tilde{l}_1 \in \mathcal{B}_1(1)$ , the codeword  $Q^n(\tilde{l}_1)$  is generated independent of  $X^n$  and according to  $\prod_{i=1}^n p_Q(q_i)$ . Note that there

are  $2^{n(r-r_1)}$  codewords in  $\mathcal{B}_1(1)$ . By packing lemma [8, Lemma 3.1], the probability term on the R.H.S. above tends to zero as  $n \rightarrow \infty$  provided  $r - r_1 \leq I(X; Q) - \delta(\epsilon')$ . Similarly,  $\Pr(\mathcal{E}_2) \rightarrow 0$  as  $n \rightarrow \infty$  if  $r - r_2 \leq I(Y; Q) - \delta(\epsilon')$ . Combining the conditions for all three events, we have  $\Pr(\mathcal{E}) \rightarrow 0$  as  $n \rightarrow \infty$  provided

$$\begin{aligned} r_1 &\geq I(Y; Q|X) + 2\delta(\epsilon'), \\ r_2 &\geq I(X; Q|Y) + 2\delta(\epsilon'). \end{aligned} \quad (56)$$

We have shown that, when (56) hold, the ensemble average of  $\Pr(\mathcal{E})$  over  $(2^{nr}, 2^{nr_1}, 2^{nr_2}, n)$  codes converges to zero as  $n \rightarrow \infty$ . Hence, we can assert that there must exist a sequence of (deterministic)  $(2^{nr}, 2^{nr_1}, 2^{nr_2}, n)$  codes such that  $\Pr(\mathcal{E}) \rightarrow 0$  as  $n \rightarrow \infty$  if (56) is satisfied. Clearly, with an appropriately small choice of  $\epsilon'$ , this sequence of codes satisfies the rate conditions (21) with  $R_1 = I(Y; U|X)$  and  $R_2 = I(X; U|Y)$ , and also the probability of error condition (22). It only remains to verify (23) which we do below:

$$\begin{aligned} &\frac{1}{n} \sum_{i=1}^n \mathbb{E}[d(X_i, Y_i, Q_i)] \\ &\leq d_{\max} \Pr(\mathcal{E}) + \mathbb{E}\left[\frac{1}{n} \sum_{i=1}^n d(X_i, Y_i, Q_i) \middle| \mathcal{E}^c\right] \\ &\leq d_{\max} \Pr(\mathcal{E}) + (1 + \epsilon') \mathbb{E}[d(X, Y, Q)], \end{aligned}$$

where the last inequality follows from the typical average lemma [8, pg. 26]. Thus, for a small enough choice of  $\epsilon'$ , we can satisfy (23) as well with  $D = D^*$ . ■

## APPENDIX C

### DETAILS OMITTED FROM SECTION IV

#### *Proof of Theorem 4.3:*

It is easy to prove this theorem from the single-letter expressions for the regions in Theorem 3.1 (along with (12)) and Theorem 4.1 by making use of the mutual information equalities (49)-(51) at the top of page 21. ■

#### *Proof of Corollary 4.4:*

$$\begin{aligned} &\sup\{R_C : R_A + R_C = H(X), \\ &\quad R_B + R_C = H(Y), (R_A, R_B, R_C) \in \mathcal{R}_{\text{GW}}\} \\ &\stackrel{(a)}{=} \sup\{R : (0, 0, I(X; Y) - R) \in \mathcal{R}'_{\text{GW}}\} \\ &\stackrel{(b)}{=} \sup\{R : (0, 0, I(X; Y) - R) \in \mathfrak{T}(X; Y)\} \\ &\stackrel{(c)}{=} C_{\text{GK}}(X; Y), \end{aligned}$$

where (a) follows from the definition  $\mathcal{R}'_{\text{GW}} = f(\mathcal{R}_{\text{GW}})$ . The  $\leq$  direction of (b) follows directly from Theorem 4.3. But  $<$  cannot hold since if  $(0, 0, I(X; Y) -$

$R) \in \mathfrak{T}(X; Y)$ , then there is a  $R' \geq R$  such that  $(0, 0, I(X; Y) - R') \in \mathcal{R}'_{\text{GW}}$ . Finally, (c) follows from Corollary 3.3.

To arrive at the alternative form, we verify the equivalence of the two forms.

$$\begin{aligned} &\{R : R \leq I(X; Y), \{R_C = R\} \cap \mathcal{L}_{\text{GW}} \subseteq \mathcal{R}_{\text{GW}}\} \\ &= \{R_C : R_A + R_C = H(X), \\ &\quad R_B + R_C = H(Y), (R_A, R_B, R_C) \in \mathcal{R}_{\text{GW}}\}. \end{aligned}$$

$\subseteq$ : if  $R \leq I(X; Y)$ , then  $(H(X) - R, H(Y) - R, R) \in \{R_C = R\} \cap \mathcal{L}_{\text{GW}}$ .

$\supseteq$ : Let  $s = (H(X) - R_C, H(Y) - R_C, R_C) \in \mathcal{R}_{\text{GW}}$ . Then (a)  $R_C \leq I(X; Y)$  since  $s \in \mathcal{L}_{\text{GW}}$ , and (b) if  $s' = (r_A, r_B, R_C) \in \mathcal{L}_{\text{GW}}$ , then since  $r_A \geq H(X) - R_C$  and  $r_B \geq H(Y) - R_C$ , we have  $s' \geq s$  (component-wise) which implies that  $s' \in \mathcal{R}_{\text{GW}}$  from the definition of the GW system. ■

#### *Proof of Corollary 4.5:*

$$\begin{aligned} C_{\text{Wyner}} &= \inf\{R_C : (R_A, R_B, R_C) \in \mathcal{R}_{\text{GW}}, \\ &\quad R_A + R_B + R_C = H(X, Y)\} \\ &\stackrel{(a)}{=} \inf\{R_1 + R_2 + I(X; Y) : (R_1, R_2, 0) \in \mathcal{R}'_{\text{GW}}\} \\ &\stackrel{(b)}{=} \inf\{R_1 + R_2 + I(X; Y) : (R_1, R_2, 0) \in \mathfrak{T}(X; Y)\}, \end{aligned}$$

where (a) follows from the definition  $\mathcal{R}'_{\text{GW}} = f(\mathcal{R}_{\text{GW}})$ ; (b) follows from Theorem 4.3:  $\geq$  direction follows directly from the theorem. But  $>$  cannot hold, since by the theorem, if  $(R_1, R_2, 0) \in \mathfrak{T}(X; Y)$  then there exists  $(R'_1, R'_2, 0) \in \mathcal{R}'_{\text{GW}}$  such that  $R'_1 \leq R_1$  and  $R'_2 \leq R_2$ . ■

#### *Proof of Corollary 4.6:*

$$\begin{aligned} &G(Y \rightarrow X) \\ &= \inf\{R_C : (H(X|Y), H(Y) - R_C, R_C) \in \mathcal{R}_{\text{GW}}\}, \\ &\stackrel{(a)}{=} \inf\{R : (R - I(X; Y), 0, 0) \in \mathcal{R}'_{\text{GW}}\} \\ &\stackrel{(b)}{=} \inf\{R : (R - I(X; Y), 0, 0) \in \mathfrak{T}(X; Y)\} \\ &\stackrel{(c)}{=} I(X; Y) + T_1^{\text{int}}(X; Y), \end{aligned}$$

where (a) follows from  $\mathcal{R}'_{\text{GW}} = f(\mathcal{R}_{\text{GW}})$ . (b) is a consequence of Theorem 4.3: And (c) follows from the definition of  $T_1^{\text{int}}(X; Y)$ .

Similarly we get (38). The equality (39) is proved in [17] which along with (37)-(38) implies (40). ■

## APPENDIX D

### DETAILS OMITTED FROM SECTION V

Here we prove Theorem 5.5. The following lemma will be useful in this.



*Lemma D.1:* Suppose  $\Pi^{(X,Y)} \xrightarrow{\epsilon} (U, V)$ . Then

$$I(\Pi_{\text{Alice}}^{\text{view}}; \Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{out}}) \leq 2\delta(\epsilon)$$

$$I(\Pi_{\text{Bob}}^{\text{view}}; \Pi_{\text{Alice}}^{\text{out}} | \Pi_{\text{Bob}}^{\text{out}}) \leq 2\delta(\epsilon)$$

where  $\delta(\epsilon) = 2H_2(\epsilon) + \epsilon \log \max\{|\mathcal{U}|, |\mathcal{V}|\}$ .

*Proof:* We show  $I(\Pi_{\text{Alice}}^{\text{view}}; \Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{out}}) \leq 2\delta(\epsilon)$  (the other relation following similarly). Let  $\Sigma_{\text{Alice}}^{\text{view}}$  be as in Definition 5.4. Then  $I(\Sigma_{\text{Alice}}^{\text{view}}; V | U) = 0$  and  $\Delta(\Sigma_{\text{Alice}}^{\text{view}} V, \Pi_{\text{Alice}}^{\text{view}} \Pi_{\text{Bob}}^{\text{out}}) \leq \epsilon$ . Also, we have  $\Delta(UV, \Pi_{\text{Alice}}^{\text{out}} \Pi_{\text{Bob}}^{\text{out}}) \leq \epsilon$ . Then

$$\begin{aligned} & I(\Pi_{\text{Alice}}^{\text{view}}; \Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{out}}) \\ &= I(\Pi_{\text{Alice}}^{\text{view}}; \Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{out}}) - I(\Sigma_{\text{Alice}}^{\text{view}}; V | U) \\ &\stackrel{(a)}{=} \left[ H(\Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{out}}) - H(V | U) \right] \\ &\quad - H(\Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{view}}) + H(V | U \Sigma_{\text{Alice}}^{\text{view}}) \\ &= \left[ H(\Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{out}}) - H(V | U) \right] \\ &\quad + \left[ H(V | \Sigma_{\text{Alice}}^{\text{view}}) - H(\Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{view}}) \right] \\ &\quad - I(V; U | \Sigma_{\text{Alice}}^{\text{view}}) \\ &\stackrel{(b)}{\leq} 2\delta(\epsilon) \end{aligned}$$

where in (a) we used  $H(\Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{view}} \Pi_{\text{Alice}}^{\text{out}}) = H(\Pi_{\text{Bob}}^{\text{out}} | \Pi_{\text{Alice}}^{\text{view}})$  (because  $\Pi_{\text{Alice}}^{\text{out}}$  is a function of  $\Pi_{\text{Alice}}^{\text{view}}$ ) and in (b) we bounded the two terms in the square brackets by invoking Lemma 2.6 twice, with  $((ABC), (A'B'C'))$  being  $((VVU), (\Pi_{\text{Bob}}^{\text{out}} \Pi_{\text{Bob}}^{\text{out}} \Pi_{\text{Alice}}^{\text{out}}))$  and  $((VV \Sigma_{\text{Alice}}^{\text{view}}), (\Pi_{\text{Bob}}^{\text{out}} \Pi_{\text{Bob}}^{\text{out}} \Pi_{\text{Alice}}^{\text{view}}))$  respectively. ■

*Proof of Theorem 5.5:* Suppose there is a protocol  $\Pi$  such that  $\Pi^{(X^{n_2}, Y^{n_2})} \xrightarrow{\epsilon} (U^{n_1}, V^{n_1})$ , for  $\frac{n_1}{n_2} \geq r - \epsilon'$ . We will denote the final views of the two parties in this protocol by  $(\Pi_{\text{Alice}}^{\text{view}}, \Pi_{\text{Bob}}^{\text{view}})$ . Also, we shall denote the outputs by  $(\Pi_{\text{Alice}}^{\text{out}}, \Pi_{\text{Bob}}^{\text{out}})$ . Then, firstly, by conditions (1) and (2) of Definition 5.2,

$$\mathcal{M}(\Pi_{\text{Alice}}^{\text{view}}; \Pi_{\text{Bob}}^{\text{view}}) \supseteq \mathcal{M}(X^{n_2}; Y^{n_2}).$$

Secondly, by Lemma D.1, for random variables  $(\Pi_{\text{Alice}}^{\text{view}}, \Pi_{\text{Alice}}^{\text{out}}, \Pi_{\text{Bob}}^{\text{out}}, \Pi_{\text{Bob}}^{\text{view}})$ , the hypothesis in condition (3') of Definition 5.6 holds, with  $\phi = \hat{\phi}(\epsilon) \cdot n_1 \cdot \log |\mathcal{U}| |\mathcal{V}|$  where we set  $\hat{\phi}(\epsilon) = 2(2H_2(\epsilon) + \epsilon)$ . Hence

$$\begin{aligned} \mathcal{M}(\Pi_{\text{Alice}}^{\text{out}}; \Pi_{\text{Bob}}^{\text{out}}) &\supseteq \mathcal{M}(\Pi_{\text{Alice}}^{\text{view}}; \Pi_{\text{Bob}}^{\text{view}}) \\ &\quad + c\hat{\phi}(\epsilon) \cdot n_1 \log |\mathcal{U}| |\mathcal{V}|, \end{aligned}$$

where  $c$  is as in Definition 5.6. Finally, since  $\Delta(U^{n_1} V^{n_1}, \Pi_{\text{Alice}}^{\text{out}} \Pi_{\text{Bob}}^{\text{out}}) \leq \epsilon$ , by the continuity of  $\mathcal{M}$  (condition (3'') of Definition 5.6), we have

$$\begin{aligned} \mathcal{M}(U^{n_1}; V^{n_1}) &\supseteq \mathcal{M}(\Pi_{\text{Alice}}^{\text{out}}; \Pi_{\text{Bob}}^{\text{out}}) \\ &\quad + \hat{\delta}(\epsilon) \cdot n_1 \log |\mathcal{U}| |\mathcal{V}|, \end{aligned}$$

where  $\hat{\delta}(\epsilon)$  is as in condition (3'') of Definition 5.6. Putting these together, after dividing throughout by  $n_1$  (using condition (4) in Definition 5.2 and convexity from condition (3'')), and using  $\frac{n_2}{n_1} \leq \frac{1}{r - \epsilon'}$ , we get

$$\mathcal{M}(U; V) \supseteq \frac{1}{r - \epsilon'} \mathcal{M}(X; Y) + \hat{\delta}'(\epsilon) \cdot \log |\mathcal{U}| |\mathcal{V}|,$$

where  $\hat{\delta}'(\epsilon) = c\hat{\phi}(\epsilon) + \hat{\delta}(\epsilon)$ .

If the rate of statistically securely sampling  $(U, V)$  from  $(X, Y)$  is  $r$ , then for all  $\epsilon, \epsilon' > 0$ , the above relation should hold. Since  $\hat{\delta}'(\epsilon) \downarrow 0$  as  $\epsilon \downarrow 0$  and the regions  $\mathcal{M}(U; V)$  and  $\mathcal{M}(X; Y)$  are closed (condition (3'')), we get

$$\mathcal{M}(U; V) \supseteq \frac{1}{r} \mathcal{M}(X; Y)$$

as required. ■